

EX 1003

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Fortinet, Inc.,

Petitioner,

v.

Netskope, Inc.,

Patent Owner.

Case No. 2025-0042

U.S. Patent 8,543,710

DECLARATION OF DR. JOHN BLACK, JR.

I, John Black, Jr. declare as follows:

I. INTRODUCTION

1. I have been retained by Fortinet, Inc. to provide analysis and opinions regarding the patentability of certain claims in U.S. Patent No. 8,543,710 ("the '710 Patent").

2. I am being compensated for my time at the rate of \$675 per hour. I have no interest in the outcome of this proceeding and the payment of my fees is in no

way contingent on my providing any particular opinions.

3. If requested, I am prepared to explain (in a deposition or at a trial before the Patent Trial and Appeal Board (the "Board")) the technology disclosed in the '710 Patent—including the state of the art in the relevant timeframe.

II. EDUCATIONAL AND PROFESSIONAL BACKGROUND

1. My qualifications can be found in my Curriculum Vitae (attached as Appendix A), which includes my detailed employment background, professional experience, and list of technical publications and patents.

2. I am an Associate Professor of Computer Science at the University of Colorado, Boulder. I received a B.S. in Mathematics and Computer Science from the California State University at Hayward (now “California State University, East Bay”) in 1988. I received an M.S. in Computer Science in 1997, and a Ph.D. in Computer Science in 2000, both from the University of California at Davis.

3. I have taught more than 60 classes in computer science, on subjects including data structures, algorithms, networking, operating systems, software engineering, security, cryptography, discrete mathematics, and quantum computing. I have authored or coauthored more than 20 publications, primarily on issues relating to computer security. I have been involved with computers and networking for over 40 years in both commercial and academic capacities.

4. My earliest interest was in networks and security. My first memories

in this regard were around 1975 when a group of friends and I learned about the telephone network and its security. A few years later, personal computers became available, and I spent most of my free time studying, programming, and modifying them. I worked extensively with various networking products throughout the 1980s, and developed an interest in cryptography soon thereafter. Although my undergraduate institution had no courses in cryptography or security in the 1980s, I decided to pursue self-study at the time, and opted to double major in Computer Science and Mathematics because cryptography is a blend of these two subject areas.

5. After earning my B.S. degree in 1988, I worked for six years at Ingres Corp as a software developer, writing and reviewing code written in C. My work primarily was directed at transaction logging, data type support, and security.

6. In 1995, I began my Ph.D. at UC Davis under cryptographer Phillip Rogaway. My area of focus was cryptography and security and my research involved encryption, authentication, hash functions, and network security.

7. After graduation I took a position as an Assistant Professor at the University of Nevada at Reno. In the Fall of 2001, I taught the networking class there, which included coverage of Ethernet, interior gateway protocols, exterior gateway protocols, ARP, DHCP/BOOTP, STP, IP, UDP, TCP, HTTP, SMTP, BGP and other protocols. In 2001, as a graduate student and I looked at the security of ARP and invented a new protocol “AuthARP” to add security to the protocol.

8. In 2002, I moved to the University of Colorado at Boulder where I am currently employed. In the Fall of 2002, I co-designed and co-taught a new course called “Foundations of Computer and Network Security,” which included descriptions of security issues around both wired and wireless security challenges, mostly for public-facing network services including the world-wide web. I have taught this class seven more times since then, including modern topics such as wireless networking, the Internet of Things, and so forth.

9. In my career at the University of Colorado, I have published several more papers in the area of cryptography and network security. I have taught more than 30 courses in network security and cryptography, and have graduated several PhD students in these areas.

10. I have also worked for a consulting company at times, writing software on contract basis. Although most projects are covered by NDAs, many involved networks and/or aspects of computer security.

11. In 2011, I began technical consulting for a local company called Cardinal Peak, which focuses primarily on video encoding and delivery systems. My work for Cardinal Peak has largely been directed to video encoding, transcoding, compression, encryption, and DRM, but also has included networking projects and embedded device work. For example, I designed the security system for the Pro1 smart thermostat, implemented the DRM for the Yonder Music App, worked on

802.1X code for smart dog collars, and helped design the cryptography used in Fitbit devices for wireless transfer of a Fitbit watch to a phone or laptop. My work has been adopted into various commercial protocols, including enterprise Wi-Fi and EMV tap-to-pay technology.

12. As part of my duties in the Computer Science department at the University of Colorado I served as chair of the Computing Committee. In 2014, I oversaw the construction of a new datacenter, including cooling, power conditioning, cabling, networking, and security for the research units within the department.

13. In 2016, I took a two-and-a-half year leave of absence from the University of Colorado to start a company named “SecureSet” in Denver, Colorado. The objective of SecureSet is to take reasonably proficient technical people and turn them into computer and network security specialists via five months of intensive training. SecureSet was sold to WeWork in 2019 and continues to offer computer security classes today. In 2018, I returned to my position at the University where I remain employed to the present day.

III. MATERIALS REVIEWED

In preparing this declaration, I reviewed and considered the following materials, along with any other materials referenced in the body of my declaration:

Exhibit	Description
1001	U.S. Patent No. 8,543,710 ("the '710 patent")

Exhibit	Description
1002	File History of the '710 patent
1004	U.S. Provisional Patent Application No. 60/551,702 ("the '702 Provisional")
1005	U.S. Patent No. 9,398,037 to Roskind et al. ("Roskind")
1006	U.S. Provisional Patent Application No. 60/613,909 to Roskind et al. ("Roskind Provisional")
1007	U.S. Patent Pub. 2003/0191966 to Gleichauf ("Gleichauf")
1008	U.S. Patent No. 6,636,894 to Short et al. ("Short")

14. I may use these documents and information, or other information obtained during the course of this proceeding, as well as representative charts, graphs, schematics and diagrams, animations, and models based on those documents and information, to support and to explain my testimony.

15. My opinions are based in part on a review and analysis of the abovementioned documents and materials. I have also drawn on my education, experience, and knowledge of basic engineering and design principles in forming my opinions.

IV. RELEVANT ART AND LEVEL OF ORDINARY SKILL

16. I have been informed that the level of ordinary skill in the relevant art at the time of the invention is relevant to inquiries such as the meaning of claim terms, the meaning of disclosures found in the prior art, and the reasons one of ordinary skill in the art may have for combining references.

17. I have been informed that factors that may be considered in determining the level of ordinary skill include: (1) the type of problems encountered in the art;

(2) prior art solutions to those problems; (3) rapidity with which innovations are made; (4) sophistication of the technology; and (5) education level of active workers in the relevant field. I have been further informed that a POSITA is also a person of ordinary creativity.

18. In my opinion, A POSITA in the field of the '710 Patent would have had either (1) at least a bachelor's degree in computer science or computer engineering or an equivalent field plus at least one year of experience working on computer networking or computer security, or (2) at least 3 years of experience working on computer networking or security, even without a formal degree.

19. At the time of the alleged invention, I was at least a POSITA in the art relevant to the '710 Patent. Further, based on my experience, I understand and know of the capabilities of a POSITA in 2005—and I am familiar with how a typical POSITA would have understood and used the terminology found in the '710 Patent and the Challenged Claims at the time of filing, and with the state of the art at that time.

20. Even though my own experience and qualifications exceed that of a POSITA, the statements herein regarding the knowledge of a POSITA and what would have been obvious to a POSITA are from the perspective of POSITA at the relevant priority date.

V. LEGAL STANDARDS APPLIED

21. I am not an attorney, but I have been informed of several legal principles, which I have employed in forming my opinions in this declaration. I have been informed that each patent claim is considered separately for purposes of patentability and that a dependent claim that depends from another claim includes all of the limitations of the claim from which it depends.

A. Burden of Proof

22. I have been informed that the petitioner in an *inter partes* review bears the burden of establishing unpatentability by "a preponderance of the evidence." I have been further informed and understand that, to prove an assertion by "a preponderance of the evidence," the party with the burden of proof must demonstrate that it is more likely than not that the assertion is true.

B. Claim Construction

23. I have been informed that the claims of the '710 Patent in this proceeding are to be construed using the same claim construction standard applied in district court. I have been informed the claim construction analysis begins with the ordinary meaning of a claim term, and there is a presumption that the term carries its plain and ordinary meaning to a person of ordinary skill in the art ("POSITA") as of the effective filing date of the patent. I have also been informed that the most important sources for determining the meaning of a claim term are the claims, the specification, and the prosecution history of the patent at issue, which collectively is

"intrinsic evidence."

1. "subordinate to"

24. The claims recite "restricting all network traffic emanating from the client device to one or more network destination addresses that are not in *or subordinate to* the first network segment," but the claims, the specification, and the file history provide no guidance or explanation as to what is meant by "subordinate to" in this context. In my opinion, a POSITA would not clearly understand the full scope of what is meant by a "network destination address[] that [is] not...subordinate to the first network segment." For example, it is unclear what sort of network address would be in a network subordinate to the first network but not also in the first network. Nonetheless, the prior art disclosures and arguments relied on herein are similar to the disclosures of the '710 patent specification. In particular, the '710 patent gives an example of restricting a client device—"client 4"—to "site 's'" (Ex. 1001, 5:35-52), which is shown in Figure 1 to be located in the general Internet. *Id.*, FIG. 1 (showing site "s" (40) in the Internet). Thus, while a POSITA would not have understood with reasonable certainty the transition point between subordinate and not subordinate in these claims, a POSITA would have understood from the specification that a general Internet website cannot be considered a network destination address that is "subordinate to the first network segment."

25. For all other terms in the '710 Patent, I have performed my analysis

using their plain and ordinary meaning to a POSITA.

C. Anticipation

26. I have been informed that a patent claim is unpatentable if it is "anticipated" by prior art. I have been informed that a reference anticipates a claim if the reference discloses each limitation of the claim at issue, either expressly or inherently. I have been informed that a prior art reference may anticipate a claim without disclosing a feature of the claimed invention if that missing characteristic is necessarily present, or inherent, in the single anticipating reference as would have been understood by a POSITA.

D. Obviousness

27. I have been informed that a patent claim is unpatentable if it would have been obvious to a POSITA at the time of the claimed invention. I have been further informed that a claimed invention is not patentable if differences between it and the prior art are such that the subject matter as a whole would have been obvious to a POSITA at the time of invention. I have been informed that factors relevant to the determination of obviousness include the scope and content of the prior art, the level of ordinary skill in the art at the time of the invention, differences between the claimed invention and the prior art, and "secondary considerations" or objective indicia of nonobviousness.

28. I have been informed that a single reference alone can render a patent

claim obvious if any differences between the reference and the claim would have been known or obvious to a POSITA at the time of the invention. That is, if the POSITA could have adapted the reference to meet the claims of the patent by applying known concepts to achieve expected results, then the patent claims are rendered obvious by that reference.

29. I have been informed that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. I have been further informed and understand that when a patent claim simply arranges old elements with each performing the same function it had been known to perform and yields no more a POSITA would expect from such an arrangement, the combination is obvious.

30. I have been informed that a patent claim composed of several limitations is not obvious merely because each limitation was independently known in the prior art. Hindsight reasoning is not an appropriate basis for combining references to form an obviousness combination. I have been further informed that it can be important to identify a reason that would have prompted a POSITA to combine multiple prior art references, or multiple teachings of the same prior art reference.

31. I have been informed that various "secondary considerations" (sometimes referred to as objective indicia of nonobviousness) may support a

determination of nonobviousness and that such secondary considerations must be considered as part of an obviousness analysis. I have been informed that even strong evidence of secondary considerations may not be sufficient to rebut a strong showing of obviousness. I have been informed that the patentee bears the burden of showing the existence and effect of secondary considerations of nonobviousness, after which the burden of coming forward with rebuttal evidence shifts to the party arguing obviousness. I have been informed that the following secondary considerations may indicate nonobviousness:

- a. Evidence that others, including the accused infringer, copied the patented invention.
- b. Evidence of a persistent problem or need in the art that was resolved by the patented invention.
- c. Evidence that others have tried and failed to solve the problem or failed to provide the need resolved by the claimed invention.
- d. The willingness of industry to license the patent at issue.
- e. Evidence that those of ordinary skill in the art were skeptical as to the merits of the invention.
- f. Evidence of praise directed to the invention by others in the field.
- g. Evidence that those of ordinary skill in the art were surprised by the capabilities of the claimed invention.

32. I have also been informed that the near-simultaneous invention by others can be evidence that a claimed invention is obvious.

33. I have further been informed that the patentee bears the burden of showing a "nexus" between the claimed invention and the evidence proffered on secondary considerations.

VI. TECHNOLOGY BACKGROUND

34. The '710 Patent deals with general networking concepts and systems that were well known and well understood as of 2004.

Overview of the Internet

35. The Internet is a global network of millions of devices. In reality, it is comprised of a large number of smaller networks that are all interconnected. Its workings are vastly complex; I will give a high-level overview of how it functions, doing my best to simplify the exposition to make an understanding of the main ideas more accessible.

Linking Devices Together

36. Every device on the Internet can, in theory, connect to any other. In order to achieve this, there must be a series of links along which information can travel from one point to another. These links can take many forms: a fiber optic link, a coax cable, a copper wire, a satellite link, a cellular link, etc. One principal design goal of the Internet is that it can operate across a wide variety of link-types, and its

success in *achieving* this is one of the reasons for the Internet's overall success.

37. Signals across all of these links occur as electromagnetic waves in various portions of the electromagnetic spectrum. These waves may operate as radio waves (through the air or inside of a wire), as optical light, or in other spectra such as infrared or microwave. All of these are part of the radio frequency spectrum and therefore communications encoded using these technologies constitute electromagnetic communications.

IP or the “Internet Protocol”

38. The Internet is a packet-switched network. All packets sent and received over the Internet are transmitted using the Internet Protocol (or “IP”)¹. In order to use the IP protocol, information is broken up into manageable chunks called “packets” and then transmitted over the various links from one device to another.

39. The IP protocol is “best effort” meaning that there is no guarantee that a particular packet will actually reach its intended destination. There are many reasons that a packet could be lost: transmission error, packet corruption, saturation of a given link, and other kinds of failures could cause a packet to be lost in transit.

IP Addresses

40. In order for a packet to be sent from one device to another using the

¹ By “IP” we mean “Internet Protocol version 4” or “IPv4” which is the format for the vast majority of Internet traffic over the last twenty years.

Internet, each must have a globally-unique IP address.² An IP address is comprised of four numbers between 1 and 255, usually written with a period separating them.

For example,

23.66.124.110

is a valid IP address written in the standard format. In fact, this address belongs to the U.S. White House.

41. Every device connected to the Internet must have an IP address.

Domain Name Service (DNS)

42. Although computers are efficient at processing information based on numbers like IP addresses, we humans often prefer more descriptive names. Instead of trying to remember the White House's IP address, 23.66.124.110, most of us would prefer www.whitehouse.gov as the website for the White House. We therefore require a service that can translate between these two designations efficiently: given a "domain name" like www.whitehouse.gov we should be able to find its IP address, and given 23.66.124.110, we should be able to recover its domain name. The service that provides this translation is called the Domain Name Service (or "DNS").

43. As stated above, every computer on the Internet *must* have a numeric

² This is once again an oversimplification. The world has run out of IP addresses and therefore we use tricks in order to allow multiple devices to share a single IP address. This would be analogous to a street running out of available addresses, and then instituting "apartment numbers" as a way to allow distinct dwellings to share a given street address provided they have different apartment numbers.

IP address, but having a DNS name is *optional*: indeed, most computers on the Internet do not have one.

HyperText Transmission Protocol (HTTP)

44. Web-based communication is commonly conducted using a protocol called the “HyperText Transmission Protocol” or “HTTP” sent over TCP/IP between a browser and a web server. Although in recent years HTTP has evolved to use UDP/IP (an alternative to TCP/IP), in 2004 the prevalent version of HTTP was 1.1 and that version used TCP/IP exclusively. I will assume HTTP version 1.1 for the purposes of this declaration.

45. The most common HTTP request from a browser is a “GET request” which is a request in plain text that starts with the word “GET” followed by a URI naming the requested resource, followed by “HTTP/1.1” indicating the version. Consider the following example for a user on the Internet who types the web site of my employer into her browser bar, “www.colorado.edu”.

46. First her browser would perform a DNS lookup to translate the name “colorado.edu” into an IP address. Next the browser would connect to that IP address using TCP/IP. Then the browser would send something like “GET http://www.colorado.edu/index.html HTTP/1.1” through the established

connection³. This message is the first appearance of the HTTP protocol in this session. The web server would then respond with an HTTP response followed by the contents of the University home page, expressed in HTML which the browser would then render.

47. A GET request can also include parameters, which are additional pieces of information appended to the URL that the server may then react to appropriately. For example, if my university had a web form that asked for my zip code, and I filled in this form and clicked on a “Submit” button, the resulting GET request might look like this:

GET http://www.colorado.edu/showmap.html?zipcode=80027

48. Here the location of the web resource ends at the “html” portion, and the remainder beginning with the question mark indicates the start of supplemental parameters.

VII. THE '710 PATENT AND PROSECUTION HISTORY

A. The '710 Patent

49. The '710 patent relates to a convention scheme for "confining a network client's network access to a specific region of the network." Ex. 1001, 1:58-60. As the specification makes clear, the purported invention simply “make[s] use of

³ In 2025, virtually every website requires encryption meaning further steps would be required to set up a TLS connection. In 2004 this was far less common and in my present example, I am not using TLS.

network firewall rule technology” to restrict client communications based on desired access control policies for the network and its users. *Id.*, 2:9–15. The patent asserts that this configuration “may offer the technical advantages of a way to reduce the negative effects of virus and worm infections” and to notify users of such infections “and offer[] a means to seek resolution.” *Id.*, 2:20–26.

50. The ’710 patent applies standard firewall rule-based techniques to isolate suspect clients. Specifically, the specification describes using known firewall functionality “to ‘quarantine’ certain clients...to particular walled garden(s)...while simultaneously allowing other clients...unhindered access to the internet.” Ex. 1001, 5:25–31. The example provided is routine: when a “computer...infected with a worm” is detected, the “gateway 11 notices the abusive traffic and ‘quarantines’ [the] client” by limiting communications to within a predefined walled garden, thereby preventing the spread of malicious traffic beyond that segment. *Id.*, 5:54–64.

51. Once quarantined, the gateway performs a redirection function commonly used in network access control systems. The patent explains that “[t]he quarantined client may then attempt to browse a web page on the Internet. In response to this attempt, the gateway redirects the web request to a cooperating web server...[which] renders a web page informing the client of its perceived infection and offering links to self-help documents and to the websites of anti-virus vendors and the client’s OS vendor.” Ex. 1001, 5:65–6:7.

52. Fundamentally, the claims are directed to (1) restricting a computer's outbound communications to specific destination addresses, and (2) further limiting those communications to designated network protocols (e.g., TCP/IP). Claim 1 is representative of the other independent claims and recites:

A method of network traffic quarantine control, comprising:

at a network access gateway device between a local network and the Internet, selecting a client device in a first network segment of the network;

at the network access gateway device, performing a plurality of quarantine control functions over the client device, wherein the plurality of quarantine control functions comprises:

a) restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment;

b) restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols; and

rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to implementation of one of the plurality of quarantine control function of the client device.

B. The '710 Prosecution History

53. The '710 patent resulted from U.S. Patent Application No. 11/076,591, filed on March 10, 2005. In its original application, the applicant submitted only three claims and all three claims were rejected as anticipated. EX1002, pp. 409-415.

Applicant subsequently tried to direct the claims to only a "walled garden" which was "in a network outside the network access gateway." *Id.*, pp. 461-467 (adding 17 more claims). The Examiner again rejected these "walled garden" claims. *Id.*, pp. 596-620. After several more rejections, Applicant cancelled all its pending claims and submitted a new set of 20 new claims for consideration. *Id.*, pp. 861-869. These too were rejected as anticipated and obvious. *Id.*, pp. 994-1004. Applicant subsequently amended the claims again to require the following underlined additions: (1) "restricting all network traffic emanating from the client device to the allowed network destination address to selected one or more network protocols"; and (2) that the web page rendering be "responsive to the implementation of one of the plurality of quarantine control function[s] of the client device." *Id.*, p. 1054. Following this amendment, the claims were allowed. *Id.*, pp. 1069-1074.

C. The '702 Provisional (EX1004) Does Not Support An Earlier Priority Date

54. I understand that, to be entitled to the benefit of the filing date of an earlier filed provisional application, the disclosure of the earlier application must provide support of the claims of the issued patent. In my opinion, the provisional application to which the '710 Patent claims priority (EX1004, "the '702 Provisional") does not provide sufficient written description support for the Challenged Claims.

55. In particular, the Challenged Claims all require "restricting all network traffic emanating from the client device to an allowed network destination address

to selected one or more network protocols." The '710 specification explains that this means that "*a network client may be constrained in terms of the types of network protocols (and applications) that they are permitted....*" Ex. 1001, 3:48-55; *see also id.*, 6:17-24 ("...all network requests from a client in network protocols *other than HTTP* are denied if they emanate from a constrained client...").

56. The '702 Provisional, however, is silent on this aspect of the claims. Nowhere in the '702 Provisional does it discuss quarantining or otherwise constraining a client such that it is limited to using only particular protocols. *See* '702 Provisional (EX1004) *generally*. Without such disclosure, I understand that the '702 Provisional cannot support an earlier priority date for the '710 patent and, accordingly, the '710 patent's priority date should be March 10, 2005, the filing date of the nonprovisional application resulting in the '710 patent.

VIII. PRIOR ART

A. U.S. Patent No. 9,398,037 to Roskind et al. (EX1005, "Roskind")

1. Overview of Roskind

57. Roskind discloses a system and method by which a gateway, such as a router, is used to "identify and intercept unauthorized, unwanted, and/or otherwise malicious communications" (Roskind, 1:14-19). The gateway is expressly "configured to provide and control access between a protected network and the Internet," and may further be used to "quarantine a local computer" when a problem is detected (Roskind, 14:27-32). Similarly, the '710 patent describes a system for

controlling access to a network based on a client's security status, emphasizing that an infected or non-compliant machine must be isolated from general network traffic. EX1001, 1:43-54 ("While the option of simply removing all network access from an abusive or abnormal client remains, business etiquette often predicates the need to constrain a client's access, rather than to remove it. Additionally, when a client device is inadvertently tainted or "infected" by a software virus or worm, the user of the client device may be unaware that the device is abnormally affecting the network. As a result, various methods to detect and limit abnormal or abusive use of network resources or connected devices have resulted in a need to establish a controlled environment in a network in order that abusive or abnormal clients can be constrained."). Both Roskind and the '710 patent thus begin from the same premise: quarantining compromised devices at the gateway to protect the integrity of the larger network.

58. Roskind provides additional detail, disclosing "a method for identifying and remedying problems.... After a detection of a problem, a computer or network containing the problem is quarantined... [wherein] quarantining includes preventing unauthorized communications from being sent from the quarantined computer..." (Roskind, 11:15-18). Roskind reiterates that "quarantining includes preventing unauthorized communications from being sent from the quarantined computer" (Roskind, 11:27-35). The '710 patent teaches the same fundamental approach—

blocking or redirecting network traffic from an infected client to prevent the spread of malicious communications (Ex. 1001, 4:34-41). In both systems, quarantine serves as an access control mechanism that halts unauthorized activity while still permitting tightly managed communication.

59. Importantly, Roskind, like the '710 patent, does not treat quarantine as a permanent denial of service but rather as a controlled state that allows remediation. Roskind explains that "access to remediation services [which] includes or may include allowing connections to servers providing security patches or advisories, for example allowing connections to a vendor's server...[or] direct access to vendor sites known to provide remediation assistance, such as to Microsoft's Windows Update service, where security patches may be obtained" (Roskind, 11:39-54). Roskind further specifies that this access is limited to certain classes of traffic—*i.e.*, certain protocols—disclosing that "access to vendor sites is restricted by the quarantine to certain classes of traffic, such as HTTP requests, certain port access, such as port 80 or port 443..." (Roskind, 11:39-54). This mirrors the disclosure of the '710 patent, which similarly provides quarantined clients with access to "a cooperating web server...[which] renders a web page informing the client of its perceived infection and offering links to self-help documents and to the websites of anti-virus vendors and the client's OS vendor" (Ex. 1001, 5:65-6:4). Both Roskind and the '710 patent therefore teach not only containment, but also guided access to remediation

resources in a restricted, secure manner.

60. Consistent with this approach, Roskind discloses redirecting unauthorized requests from a quarantined client to "a special quarantine server, such as an ISP web server that provides information and links to assist in remediation" (Roskind, 14:66-15:1). Roskind elaborates that "the server responds with a quarantine notification page (1604)...a web page that provides notification that the computer is quarantined, and/or provides links to remediation sites appropriate to the quarantine, such as a link to a site that provides anti-contagion software for removing a virus..." (Roskind, 15:57-16:43). This is directly analogous to the '710 patent's disclosure of redirecting users to a cooperating web server that provides infection notifications and links to relevant remediation sites (Ex. 1001, 5:65-6:4). In both systems, redirection functions as the mechanism by which quarantined clients are simultaneously informed of their condition and given the tools to remediate it.

61. Roskind also extends its teachings by describing continuous monitoring of both network traffic and individual computers. First, Roskind discloses monitoring network traffic to detect malicious activity (Roskind, 13:10-53). Second, Roskind teaches monitoring specific computers for infestation through a "query for cleanliness," which may be answered by anti-contagion software with "assertions about the currency of a scan...wherein a sufficiently updated software and/or scan

may act as a cleanliness assertion" (Roskind, 13:54-14:26). This corresponds closely to the '710 patent's discussion of determining whether a client satisfies compliance checks before allowing unrestricted access (Ex. 1001, 3:34-46). In both disclosures, the system monitors client health, and upon sufficient assurance of cleanliness or compliance, the client is permitted to exit quarantine and regain normal access.

62. A POSITA would therefore have understood Roskind to teach the same core principles set out in the '710 patent: (i) quarantining infected devices at the network gateway, (ii) blocking unauthorized communications while permitting controlled access to remediation resources, (iii) redirecting clients to specialized servers that provide remediation assistance, and (iv) restoring full network participation once the client has demonstrated its cleanliness or compliance. Roskind provides detailed implementation of these steps, including specific disclosures about quarantine servers, remediation access, and cleanliness assertions, which align directly with the '710 patent's disclosure of cooperating web servers, remediation links, and compliance checks. Together, the two references reinforce a consistent model of network access control that isolates threats while enabling remediation and eventual reintegration of the client into the trusted network.

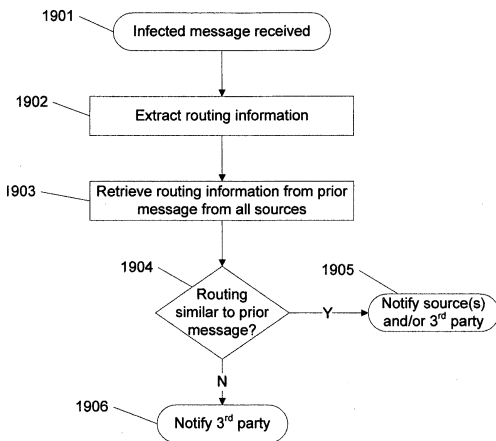
2. Roskind's Provisional Application Supports An Earlier Priority Date

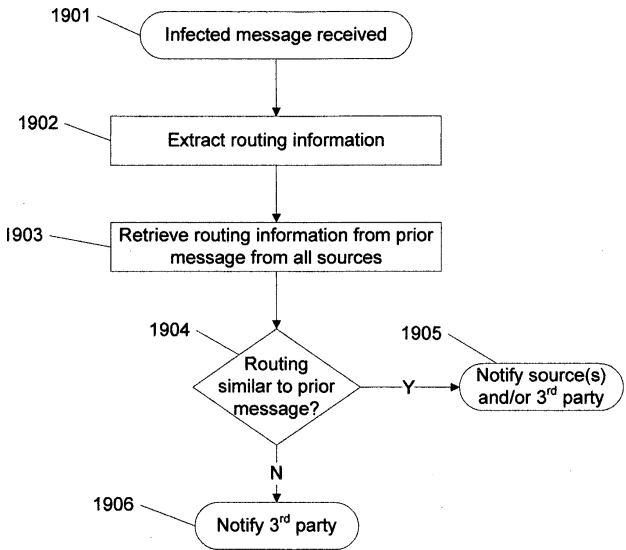
63. I understand that a prior art patent that is filed *after* the priority date of the challenged patent (here, the '710 patent) may still be considered prior art to the

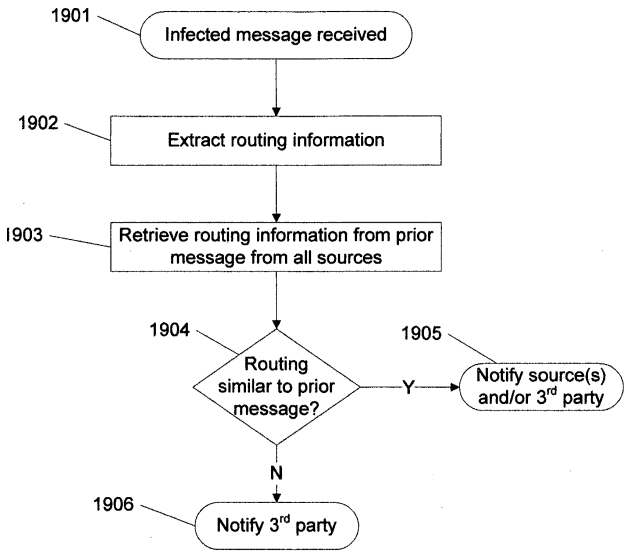
challenged patent if the prior art reference claims priority back to a provisional application filed *before* the challenged patent's priority date. I further understand that to be entitled to this earlier priority date, two conditions must be met: (1) the priority document (e.g., the provisional application) must support at least one claim of the issued prior art patent; and (2) the priority document must support the disclosures relied upon to invalidate the challenged patent. In my opinion, Roskind satisfies these conditions and is therefore prior art to the '710 Patent.

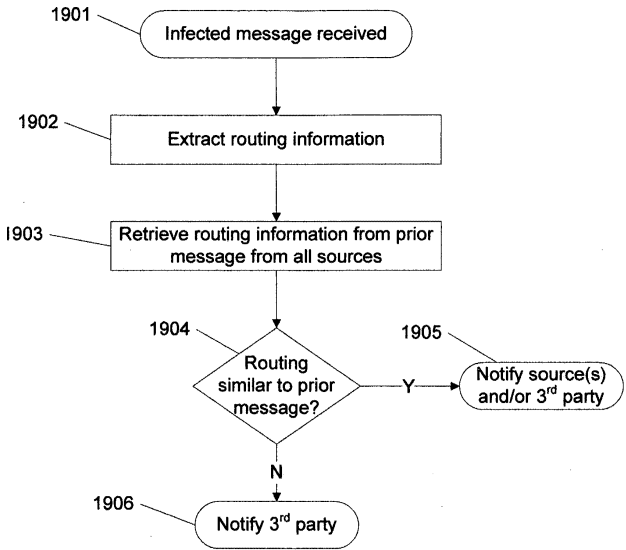
64. As cited throughout my analysis of the '710 claims herein, the Roskind Provisional (EX1006) includes with minor exceptions the very same disclosures relied upon in Roskind and therefore meets the second condition above. In addition, as set forth in the table below, the Roskind Provisional includes written description support for claim 1 of Roskind, as issued:

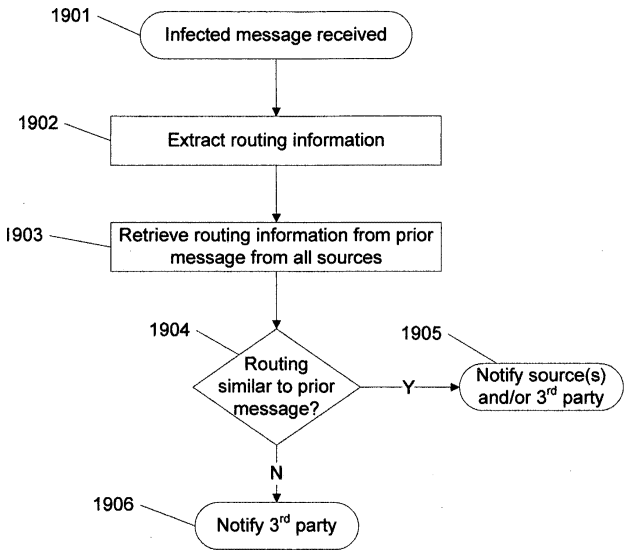
Claim 1 of Roskind (EX1005)	Roskind Provisional (EX1006)
[1.pre] A method, comprising	4:1-5 (disclosing "a process").
[1.1] determining that a received network communication is classified by anti-contagion software as infected;	33:20-34:2 ("FIG 19 is a flow diagram of a method for notifying possible sources of infection according to some embodiments. In this example, an infected message is received (1901). An example of <i>an infected message</i> is <i>a message classified as such by anti-contagion software.</i> ")
[1.2] extracting first routing information from the received network communication;	34:1-7 (" <i>Routing information may be extracted from the message</i> (1902). . .")
[1.3] determining whether	34:7-21 ("Routing information from previously

Claim 1 of Roskind (EX1005)	Roskind Provisional (EX1006)
second routing information from a prior network communication received previously matches the first routing information; and	received messages may be retrieved (1903).... <i>Routing information for the infected message may be compared with the retrieved routing information (1904). If no similarity with previous messages is found (1904) then third party notification is optionally made.... If a similarity is found with previous messages (1904) then a notification may be sent (1905) in this example...."</i>) FIG 19 (1904):  <pre> graph TD 1901([1901: Infected message received]) --> 1902[1902: Extract routing information] 1902 --> 1903[1903: Retrieve routing information from prior message from all sources] 1903 --> 1904{1904: Routing similar to prior message?} 1904 -- Y --> 1905([1905: Notify source(s) and/or 3rd party]) 1904 -- N --> 1906([1906: Notify 3rd party]) </pre> Figure 19
[1.4a] sending a notification that the received network communication was classified as infected,	33:20-21 ("FIG 19 is a flow diagram of a method for <i>notifying possible sources of infection</i> according to some embodiments.") FIG 19 (1905, 1906):

Claim 1 of Roskind (EX1005)	Roskind Provisional (EX1006)
	 <pre> graph TD 1901([1901 Infected message received]) --> 1902[1902 Extract routing information] 1902 --> 1903[1903 Retrieve routing information from prior message from all sources] 1903 --> 1904{1904 Routing similar to prior message?} 1904 -- Y --> 1905([1905 Notify source(s) and/or 3rd party]) 1904 -- N --> 1906([1906 Notify 3rd party]) </pre> Figure 19
[1.4b] wherein the notification is sent to a recipient selected from the group consisting of a sender associated with the prior network communication and a third party, wherein the third party is not a sender of the prior network communication and wherein the third party is not a sender of the received network communication,	34:12-35:7 ("If no similarity with previous message is found (1904) then third party notification is optionally made (1906) in this example. An example of a third party notification is sending notification to the ISP that provides network access to the message source. Another example of notifying a third party is notifying a viral clearinghouse of the apparent source of a viral message. Another example of a notifying a third party is notifying a collaborative filter service... [N]otification may be sent (1905) to one or more sources of the prior message(s) that best match the infected message, and/or to third parties...") FIG 19 (1905, 1906):

Claim 1 of Roskind (EX1005)	Roskind Provisional (EX1006)
	 <pre> graph TD 1901([1901 Infected message received]) --> 1902[1902 Extract routing information] 1902 --> 1903[1903 Retrieve routing information from prior message from all sources] 1903 --> 1904{1904 Routing similar to prior message?} 1904 -- Y --> 1905([1905 Notify source(s) and/or 3rd party]) 1904 -- N --> 1906([1906 Notify 3rd party]) </pre> Figure 19
[1.4c] wherein the recipient is selected as the sender associated with the prior network communication if it is determined that the first routing information and the second routing information match,	34:13-35:3 ("Routing information for the infected message may be compared with the retrieved routing information (1904).... If <i>a similarity is found with previous message</i> (1904) then a notification may be sent (1905) in this example.... [N]otification may be sent (1905) to one or more sources of the prior message(s) that best match the infected message...")

Claim 1 of Roskind (EX1005)	Roskind Provisional (EX1006)
	FIG 19 (1905):  <pre> graph TD 1901([1901: Infected message received]) --> 1902[1902: Extract routing information] 1902 --> 1903[1903: Retrieve routing information from prior message from all sources] 1903 --> 1904{1904: Routing similar to prior message?} 1904 -- Y --> 1905([1905: Notify source(s) and/or 3rd party]) 1904 -- N --> 1906([1906: Notify 3rd party]) </pre> Figure 19
[1.4d] and wherein the recipient is selected as the third party if it is not determined that the first routing information and the second routing information match.	34:13-15 ("Routing information for the infected message may be compared with the retrieved routing information (1904). <i>If no similarity with previous messages is found (1904) then third party notification is optionally made (1906) in this example.</i>") FIG 19 (1906):

Claim 1 of Roskind (EX1005)	Roskind Provisional (EX1006)
	 <pre> graph TD 1901([1901 Infected message received]) --> 1902[1902 Extract routing information] 1902 --> 1903[1903 Retrieve routing information from prior message from all sources] 1903 --> 1904{1904 Routing similar to prior message?} 1904 -- Y --> 1905([1905 Notify source(s) and/or 3rd party]) 1904 -- N --> 1906([1906 Notify 3rd party]) </pre> Figure 19

65. Accordingly, I understand that Roskind is entitled to the September 27, 2004 priority date of the Roskind Provisional and is therefore prior art to the '710 patent (which itself was filed only in March 2005).⁴

B. U.S. Patent Pub. 2003/0191966 to Gleichauf (EX1007, "Gleichauf")

66. Gleichauf describes a system and method designed “for detecting an infective element in a network environment” (Gleichauf, Abstract, ¶ 20). A key

⁴ As explained above, in my opinion, the '710 patent is not entitled to the March 2004 priority date of the '702 Provisional. *Supra* § VII.C.

aspect of this system is its use of community-based monitoring within the network, which allows only a portion of the nodes to be correctly configured in order to detect a malicious entity. As Gleichauf notes, this method of “community monitoring” enables swift quarantining of harmful traffic once it's identified, which is especially important in cybersecurity scenarios where rapid containment of a threat is crucial (Gleichauf, ¶ 20). In this respect, Gleichauf emphasizes rapid isolation of compromised or hostile components as a core protective measure—an approach also found in the '710 patent.

67. Gleichauf specifically states that the quarantining capability is managed by a “network management controller,” which enables the system to isolate malicious traffic as soon as it is detected within the network (Gleichauf, ¶ 6). According to Gleichauf, the controller can take various corrective actions in response to the identification of an infective element, aiming to prevent it from spreading throughout the vulnerable system (Gleichauf, ¶ 20). Among the measures described are: (a) “immediately disabl[ing] the communications capability” of a compromised or rogue device to stop it from reaching other machines or destinations—thus avoiding further infection—while simultaneously rerouting the device to a remediation website that enforces compliance with network security protocols (Gleichauf, ¶¶ 6, 8); and (b) applying access restrictions by using a “policies node” to disable certain services or functions on the infected device until

it meets the required security criteria (Gleichauf, ¶¶ 6, 8, 58). Through these mechanisms, Gleichauf—like the '710 patent—illustrates a quarantine approach that does not entirely sever network connectivity. Instead, the infected device is placed in a restricted state that permits only the minimal communication necessary to connect with remediation infrastructure, such as limited TCP/IP traffic. In both disclosures, then, quarantine is portrayed as a controlled redirection rather than a complete network blackout.

68. I understand that Patent Owner may argue that Gleichauf's reference to a "remediator website" implies it must reside within the same internal network. In my opinion, however, a POSITA would have recognized that the location of such a resource—whether internal or external—is simply a matter of design preference. Gleichauf clarifies that the term "internal network" can refer to configurations such as a LAN, WAN, or MAN (Gleichauf, ¶ 50). In my opinion, a POSITA would have understood that hosting the remediation site on the Internet would still meet the criteria of being outside—or not subordinate to—the infected machine's original network segment. For instance, a compromised device on a home network or enterprise subnet could easily be redirected to an Internet-based remediation site. Such a configuration would have been an obvious and routine variation for someone skilled in the art.

69. Gleichauf further describes the use of a "signal" as part of the

mechanism for detecting and responding to an infected computer within the network (Gleichauf, ¶ 5). This signal can be sent either to or from the network management controller (*id.*, ¶ 7), and in some instances, is transmitted “directly to [the] infected computer” (*id.*, ¶ 45). The specification provides additional detail, noting that the signal contains multiple pieces of information related to the identified infective element. For instance, the signal may specify the type of malicious component that has infiltrated the system and may also convey remedial instructions tailored to addressing that particular threat. In some cases, the threat may be neutralized through a simple deletion command, while others may require more involved guidance. Alternatively, the signal may carry any other type of information that assists in managing or mitigating the effects of the infective element (Gleichauf, ¶ 48).

70. It is my opinion that a POSITA reviewing Gleichauf’s disclosures would have understood the referenced “signal” as a structured method for delivering information—such as a web page or a similar communication—sent to the infected machine. From a practical standpoint, a POSITA would have readily seen the utility and obviousness of using such a signal to serve a web page in response to the user’s attempts to access other network destinations. In this scenario, while the system restricts the infected computer’s communication capabilities, it could also provide immediate feedback to the user explaining the reason for the failure and offering remediation guidance. This approach would have been both user-friendly and

technically straightforward to implement, relying on established web technologies available at the time.

71. Thus, Gleichauf—like the '710 patent—describes a network security system that: (i) identifies and quarantines infected machines; (ii) limits their ability to communicate in order to contain the threat; (iii) redirects them to a remediation site that can be accessed only through restricted network protocols; and (iv) delivers remediation guidance to the user via a structured signal. In my opinion, a POSITA would have viewed these features as consistent with and complementary to those in the '710 patent and would have readily understood how to implement them using conventional techniques.

C. U.S. Patent No. 6,636,894 to Short et al. (EX1008, "Short")

72. Short describes a gateway device that acts as a key interface connecting users to various networks and online services. According to Short, this device “serves as an interface connecting [a] user to a number of networks or other online services,” including, for instance, the Internet, an enterprise network, or other types of networked systems (Short, 2:5–9). In this role, the gateway enables Internet Service Providers (ISPs) and enterprise network operators—such as those managing LANs in environments like hotels—to offer users a simple and seamless way to access both local networks and external online services (Short, 2:45–50).

73. To enable user access, Short explains that service providers may

“redirect users to portal pages that [they]...wish the user to access or view” (Short, 2:51–53). These portal pages may include, for instance, a “login page” where users can enter their credentials to be authenticated and granted network access (Short, 3:9–12). Notably, Short also discloses that the portal page “can...be maintained on a server local to the gateway device” (Short, 5:32–34). In fact, the specification underscores this point multiple times, describing that the process may involve “establishing a login page on a webserver local to the gateway device prior to redirecting the user to the login page,” and further detailing that the user’s login information is collected and then used by the gateway to control access to the destination network (Short, 4:13–21). Short reiterates this local hosting capability, noting that the “login page is maintained local to the gateway device” (*id.*, 4:54–55).

74. Short explicitly outlines the benefits of hosting the web server locally within the gateway device, noting that this configuration makes redirection “efficient and fast” (Short, 9:5–15). Additionally, Short teaches that redirection can be selectively applied to specific types of traffic—for example, limiting it to web page requests while excluding other forms of data such as email, FTP, or other network traffic (Short, 9:26–48).

75. Short also emphasizes the adaptability of the portal page, explaining that it “can be a webpage containing any information whatsoever” and may be created by the ISP, the enterprise network administrator, or even the user.

Furthermore, the portal page can display information tailored to the specific user accessing the network (Short, 8:20–30). These portal pages might also include commercial or service-related promotions, such as offers connected to the network service provider itself (Short, 10:5–19). Consistent with this, Short notes that users are directed to a login page where they must enter their credentials to gain access to the network (*id.*, 4:54–59).

76. Short clearly states that the login page hosted on the local web server “accept[s] user information...which is thereafter utilized by the gateway device to authorize the user access to the destination address...which can be an Internet destination address” (Short, 4:22–25). Put differently, Short explicitly teaches the concept of “rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet.”

IX. SUMMARY OF OPINIONS

77. I have been asked to compare the references cited herein to claims 1-20 of the '710 patent (the "Challenged Claims").

a. Grounds 1 and 2: In my opinion, claims 1-20 are anticipated by, and at minimum rendered obvious over Roskind.

b. Ground 3 and 4: In my opinion, claims 1-20 are anticipated by, and at minimum rendered obvious over Gleichauf.

c. Ground 5: In my opinion, claims 1-20 are obvious over Roskind in view of Short.

d. Ground 6: In my opinion, claims 1-20 are obvious over Gleichauf in view of Short.

X. GROUNDS 1 AND 2 - ROSKIND

A. Independent Claim 1

1. Claim 1[pre]: "A method of network traffic quarantine control, comprising:"

78. In my opinion, Roskind discloses this limitation. Roskind discloses a method of network traffic quarantine control.

79. Roskind address the problem that "[u]nwanted and/or malicious network communications . . . burden affected networks with unauthorized and/or undesired traffic." Roskind, 1:14–19. Roskind solves this problem by "[a]nalyzing routing information to identify and intercept unauthorized, unwanted, and/or otherwise malicious communications[.]" *Id.*, Abstract. Roskind confirms its "invention can be implemented in numerous ways, including as a process" (*id.*, 2:47-52).

80. Roskind further discloses that, once such communications or problems are identified, the system may "quarantine" the affected computer or network. *Id.*, 11:15-18. Specifically, Roskind teaches:

"FIG. 10A is a flow diagram of a method for identifying and remedying problems.... After a detection of a problem, a computer or network

containing the problem is quarantined...quarantining includes preventing unauthorized communications from being sent from the quarantined computer.... Examples of quarantining activities are illustrated in FIGS. 14 and 15."

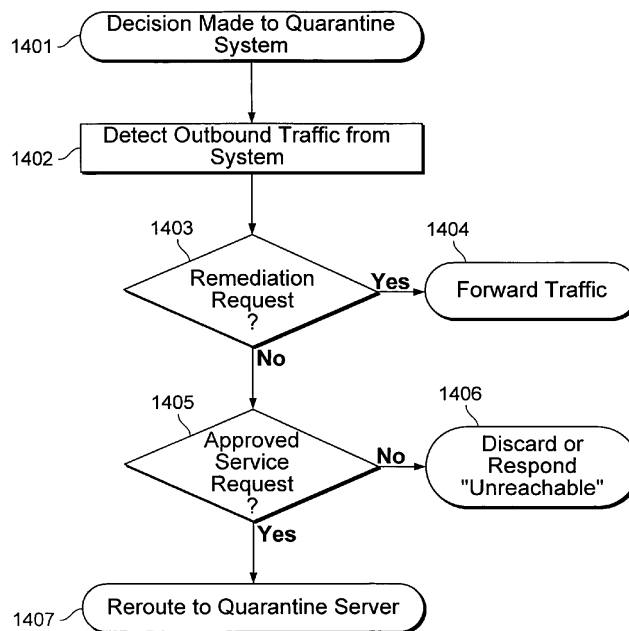


FIG. 14

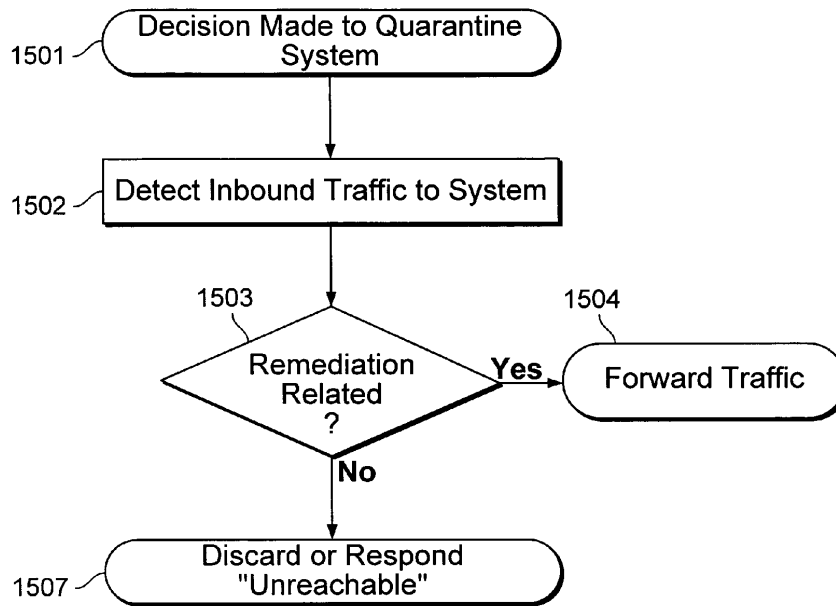


FIG. 15

Roskind, FIGs. 14-15; see also, Ex. 1006, 4:1-5, 18:7-19:3.

2. Claim 1[a]: "at a network access gateway device between a local network and the Internet, selecting a client device in a first network segment of the network;"

81. In my opinion, Roskind discloses this limitation. Roskind discloses, or at minimum renders obvious, at a network access gateway device (e.g., "router") between a local network (e.g., "LAN") and the Internet, selecting (e.g., "deciding to quarantine") a client device (e.g., "host", "local computer") in a first network segment of the network (e.g., "LAN").

82. Roskind discloses a "gateway 1028...configured to provide and control access between a protected network and the Internet," which incorporates, or may itself be, a "router." *See, e.g.*, Roskind, 11:57–12:3 ("FIG. 10B is a block diagram

illustrating a network environment in which infected hosts and/or networks are quarantined.... A plurality of hosts 1 to 'm', represented in FIG. 10B by hosts 1020, 1022, and 1024, connect via a router 1026 and a gateway 1028 to the Internet 1030.... [R]outer 1026 is omitted or included in the gateway 1028.... [G]ateway 1028 comprises a gateway, router, firewall, or other device configured to provide and control access between a protected network and the Internet....").

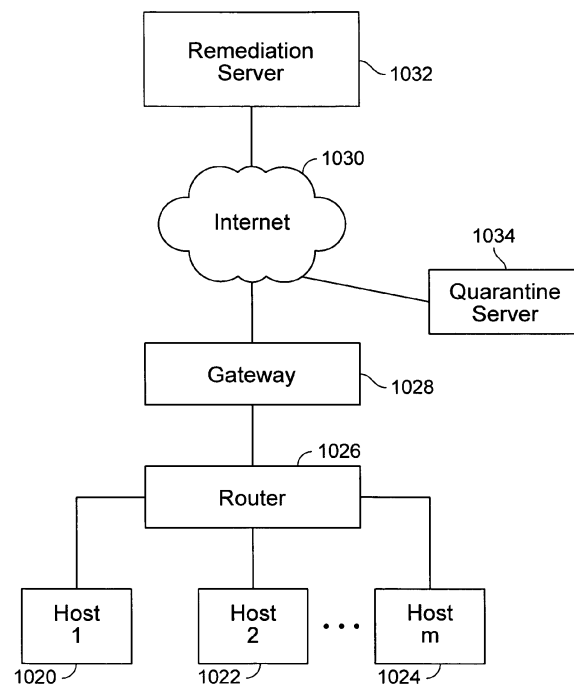


FIG. 10B

83. Roskind further teaches that the quarantine process is initiated when a "firewall or router for a LAN decid[es] to quarantine a local computer." Roskind, 14:27–32 ("FIG. 14 is a flow diagram of a method for quarantining a computer.... In this example, a decision has been made to quarantine a computer (1401), such

as...a firewall or router for a LAN deciding to quarantine a local computer."); Ex. 1006, 24:13–17.

84. The Roskind Provisional is consistent, disclosing a "router for a LAN deciding to quarantine a local computer" and describing the resulting quarantine as "restricting internet connections," thereby confirming the router functions as the network access gateway between the LAN and the Internet. Ex. 1006, 24:13–17, 27:4–10 ("a configuration based quarantines...may be automatically setup...that establishes a quarantine, for example restricting internet connections...."). Based on these disclosures, a POSITA would therefore have understood that Roskind—and at minimum Roskind's Provisional—expressly teaches or renders obvious a router operating as a network access gateway device between a local network and the Internet so as to "restrict[] internet connections" between the device in the first segment of the network (the LAN) and the Internet.

85. Figure 14 illustrates the operation of this process once the router has "decid[ed] to quarantine a local computer," i.e., a host within the first network segment (the LAN):

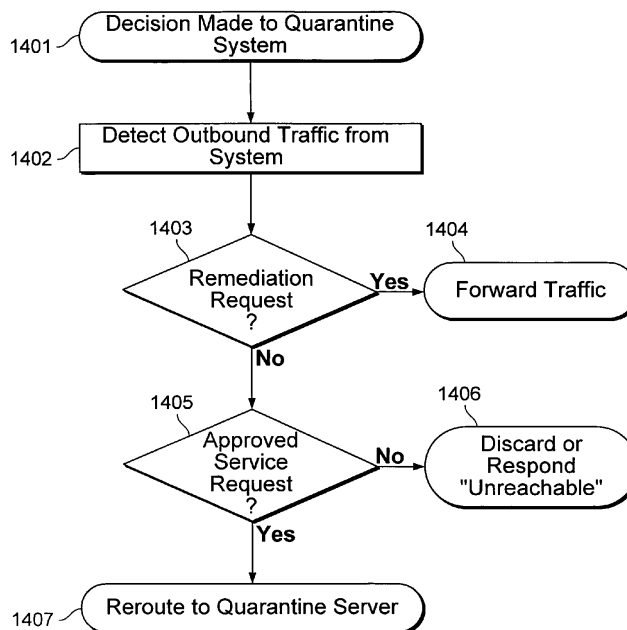


FIG. 14

Roskind, FIG. 14.

3. Claim 1[b]: "at the network access gateway device, performing a plurality of quarantine control functions over the client device, wherein the plurality of quarantine control functions comprises:"

86. In my opinion, Roskind discloses this limitation. Roskind discloses at the network access gateway device (e.g., "router"), performing a plurality of quarantine control functions over the client device(e.g., "quarantining a computer"), wherein the plurality of quarantine control functions comprises [[1b(a)]-[1b(b)]].

87. Roskind discloses that a "firewall or router for a LAN" may decide to quarantine a computer. *See, e.g.*, Roskind, 14:27–50 ("FIG. 14 is a flow diagram of a method for quarantining a computer.... [A] decision has been made to quarantine a computer (1401), such as...a firewall or router for a LAN deciding to quarantine

a local computer."). This quarantine may be in response to the router, firewall, or other network component detecting a vulnerability or infestation. *See, e.g., Roskind, 11:15–39 ("FIG. 10A is a flow diagram of a method for identifying and remedying problems...detection may be made by a router, firewall, or other network component.... After a detection of a problem, a computer or network containing the problem is quarantined (1002). In some embodiments, quarantining includes preventing unauthorized communications from being sent from the quarantined computer, ..., or efforts to communicate data without authorization.... In some embodiments, quarantining includes preventing undesired communications from reaching the quarantined computer, such as control messages or infectious messages. Examples of quarantining activities are illustrated in FIGS. 14 and 15.").*

88. For instance, Figure 10A depicts "a method for identifying and remedying problems," including step 1002 ("a computer or network containing the problem is quarantined"). Roskind, 11:15-39.

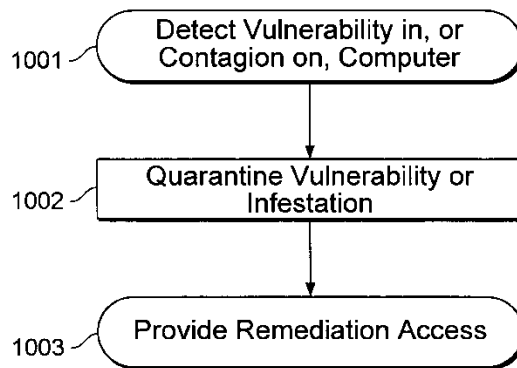


FIG. 10A

89. Figures 14 and 15 illustrate "examples of quarantining activities":

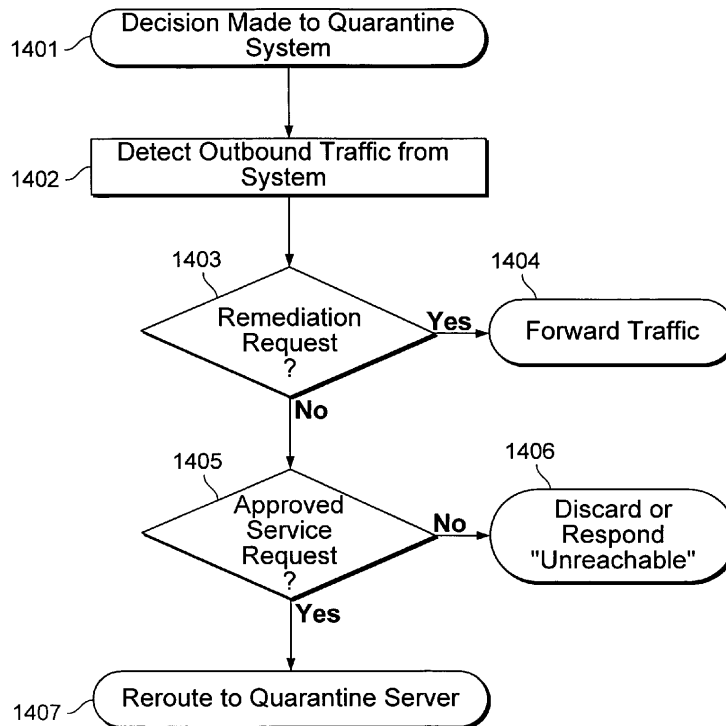


FIG. 14

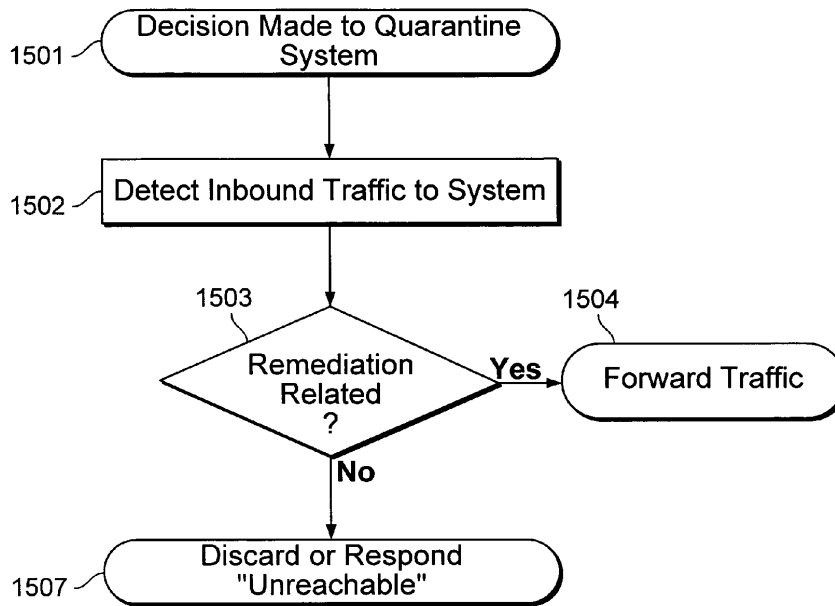


FIG. 15

Roskind, FIGs. 10A, 14, 15; see also Ex. 1006, 24:13–17, 18:7–18:3.

4. Claim 1[b(a)]: "restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment;"

90. In my opinion, Roskind discloses this limitation. Roskind discloses, or at minimum renders obvious, restricting all network traffic emanating from the client device (e.g., "preventing unauthorized communications from being sent from the quarantined computer") to one or more network destination addresses that are not in or subordinate to⁵ the first network segment (e.g., restricting "outbound traffic" not "associated with a remediation request").

⁵ In my opinion, this limitation is met by destinations "that are not in...the first network segment" without addressing the phrase "or subordinate to."

91. Roskind teaches that following the quarantine of a computer or network, unauthorized communications are prevented, while restricted access is maintained to designated “remediation” services, which is shown in Figure 15 below.

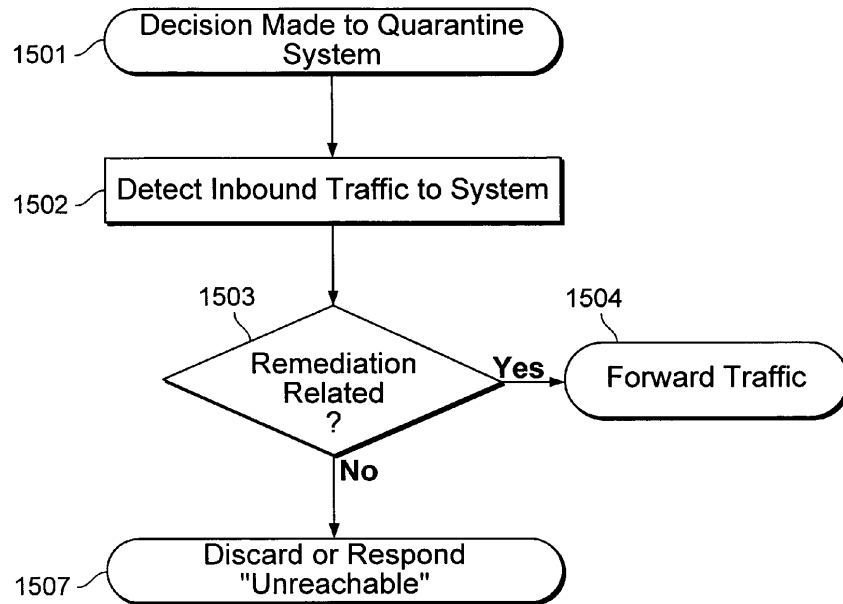


FIG. 15

92. Roskind explains that “quarantining includes preventing unauthorized communications from being sent from the quarantined computer, such as efforts to infect, probe, or harass other computers, or efforts to communicate data without authorization” (Roskind, 11:27–35). In certain embodiments, no communications are permitted at all (*id.*).

93. Roskind discloses that network traffic from a quarantined client device is restricted to permit only communications directed toward designated

“remediation” services. Specifically, Roskind states that “the quarantined computer is provided access to remediation services (1003).... [A]ccess to remediation includes or may include allowing connections to servers providing security patches...such as to Microsoft’s Windows Update service, where security patches may be obtained” (*id.*, 11:39–50). Moreover, Roskind clarifies that “access to vendor sites is restricted by the quarantine to...certain content requests, such as specific URLs” (*id.*, 11:50–54). These remediation servers—such as those operated by anti-contagion software distributors or security patch providers—are necessarily located on separate network segments from the quarantined device, and are on a different network altogether than the quarantined client, as the client is on the local network and the remediation servers are on the Internet. Consequently, because these servers are on the Internet, a POSITA would have understood them to not be subordinate to the quarantined client’s local network (*see id.*, 14:50–15:12). I note that this is consistent with the ’710 patent’s disclosure of restricting a client device to access only an Internet “site ‘s’” (Ex. 1001, 5:35–52, FIG. 1 (40)).

94. Roskind additionally discloses filtering network traffic during quarantine to permit only authorized communications related to remediation. For instance, Figure 14 illustrates a process where “outbound traffic is detected (1402)...[and] tested...to see if it is associated with a remediation request (1403), such as contact with an appropriate anti-contagion software distributor, or contact

with a security patch update provider” (Roskind, 14:50–56).

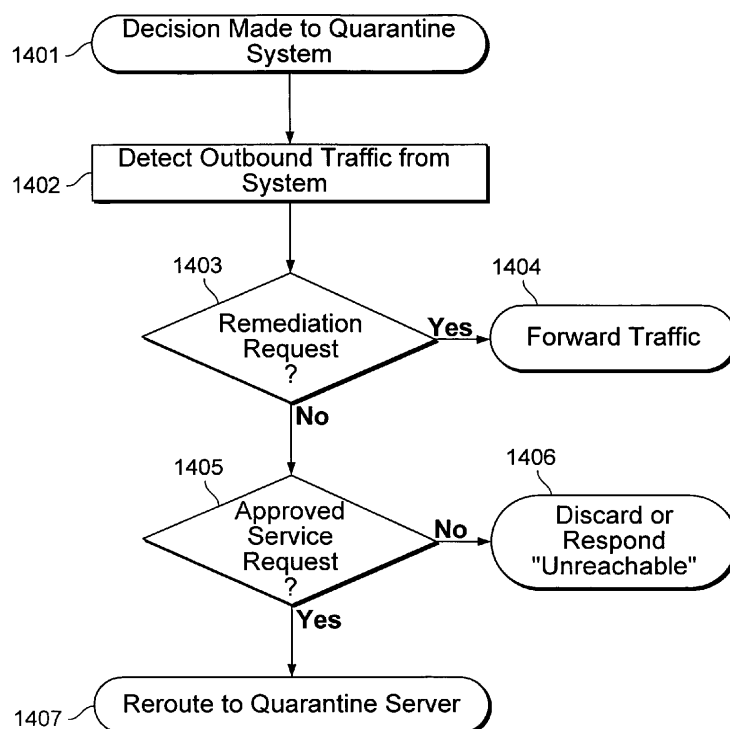


FIG. 14

95. If the outbound traffic is not linked to remediation, it is further examined to determine whether it qualifies as an “approved service request (1405), such as a request for a web page” (*id.*, 14:56–59). When a request matches an approved service, it is then “re-routed to a special quarantine server (1407),” effectively limiting the quarantined computer’s access to the intended service (*id.*, 14:59–61). Conversely, if the request does not correspond to an approved service, “the outbound traffic is discarded or responded to with [an] indication that the desired traffic destination is unreachable” (*id.*, 15:1–6). Thus, Roskind clearly

teaches a quarantine system that (i) blocks unauthorized communications, (ii) allows access exclusively to remediation services identified by specific URLs associated with security patch providers, and (iii) restricts or rejects all other outbound traffic, including requests for otherwise permitted services. *See also* Ex. 1006, 25:8–26:8, 19:4–15, 18:16–22.

5. Claim 1b(b): "restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols;"

96. In my opinion, Roskind discloses this limitation. Roskind discloses, or at minimum renders obvious, restricting all network traffic emanating from the client device ("preventing unauthorized communications from being sent from the quarantined computer") to an allowed network destination address ("vendor sites") to selected one or more network protocols ("HTTP requests").

97. Roskind teaches that even when a quarantined computer is permitted to access remediation services—such as “vendor sites”—that access is further limited to specific categories of traffic, for example, “HTTP requests.” As Roskind explains, “[t]he quarantined computer is provided access to remediation services (1003).... [A]ccess to remediation includes...allowing connections to servers providing security patches or advisories, for example...a vendor’s server.... [A]ccess to remediation includes allowing direct access to vendor sites known to provide remediation assistance...where security patches may be obtained. In some

embodiments, access to vendor sites is restricted by the quarantine to certain classes of traffic, such as HTTP requests, certain port access, such as port 80 or port 443, ...” (Roskind, 11:39–56); *see also* Ex. 1006, 19:14–15. Accordingly, all other types of traffic—that is, other network protocols—are blocked.

6. Claim 1[c]: "and rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to implementation of one of the plurality of quarantine control function of the client device."

98. In my opinion, Roskind discloses this limitation. Roskind discloses, or at minimum renders obvious, rendering a web page ("quarantine notification page") to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet ("information and links to assist in remediation"; "remediation information", "notification that the computer is quarantined[and] links to remediation sites appropriate to the quarantine") responsive to implementation of one of the plurality of quarantine control function of the client device ("web page...[or]...remediation sites appropriate to the quarantine").

99. **rendering a web page to display on the client device from the network access gateway device** - Roskind specifically discloses that a quarantined computer’s browser can be redirected to a “quarantine server.” As described, the

client system includes “browser software used to navigate the World Wide Web, e.g., to send/receive data to/from a website” (Roskind, 7:2–13). Furthermore, Roskind explains that “the request is re-routed to a special quarantine server (1407), such as an ISP web server that provides information and links to assist in remediation” (*id.*, 14:66–15:1). Additionally, Figure 4B depicts a client system configured to obtain updates, where the “update agent/browser 424 comprises browser software used to navigate the World Wide Web, e.g., to send/receive data to/from a website from which an update is available for download” (*id.*, 6:63–7:23).

100. Roskind discloses that the quarantine server “respond[s] to requests...with a quarantine notification page (1604)...a web page that provides notification that the computer is quarantined, and/or provides links to remediation sites appropriate to the quarantine, such as a link to a site that provides anti-contagion software for removing a virus that the quarantined computer is believed to contain” (Roskind, 15:57–16:43). Additionally, Roskind teaches that the quarantine server “resides on the router...and/or gateway” (*id.*, 11:57–12:13), and describes the “special quarantine server” as “an ISP web server” (*id.*, 14:65–15:1). At a minimum, a person having ordinary skill in the art (POSITA) would have understood—and found it an obvious design choice—to position the quarantine server within the gateway to better manage infected traffic while preventing the quarantined computer from communicating with unauthorized hosts. For instance, Roskind’s suggestion of

using an ISP web server as the quarantine server—that is, having the entity controlling Internet access also provide the quarantine server—demonstrates this advantage for an organization aiming to protect its network. Furthermore, if “rendering” the web page involves generating the complete page at the server rather than on the local browser (and providing that completely rendered page to the client), this too would have been an obvious and straightforward design decision. As a POSITA would have understood, there are only two options—server-side or client-side rendering—and Roskind’s disclosure that the quarantine server “respond[s] to requests...with a web page that provides notification that the computer is quarantined” (*id.*, 15:57–16:43) supports both approaches. Indeed, the specific location of graphically “rendering” a web page is not the invention’s focus nor a detailed aspect of the ’710 specification, and both options would have been well known and obvious to a POSITA. Further, a POSITA would have understood benefits of generating a remediation page at the server so as to reduce processing time and power and ensure the page could be retrieved and properly viewed by a multitude of client devices using varied software.

101. wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to implementation of one of the plurality of quarantine control function of the client device - Roskind further explains that the “re-rout[ing] to a

special quarantine server” occurs as part of the “method for quarantining a computer,” specifically in response to the gateway restricting access to any sites beyond the designated remediation sites (Roskind, 14:27–15:12, FIG. 14). Figure 16 provides additional details on the quarantine server’s response to requests, noting that the server “responds with a quarantine notification page (1604),” which is a web page “that provides notification that the computer is quarantined, and/or provides links to remediation sites appropriate to the quarantine, such as a link to a site that provides anti-contagion software for removing a virus that the quarantined computer is believed to contain” (Roskind, 15:57–16:9). Roskind also discloses that “access to remediation includes or may include allowing connections to servers providing security patches or advisories, for example allowing connections to a vendor’s server, or providing virus and worm disinfecting tools, such as focused removal tools” (*id.*, 11:41–50).

102. Moreover, Roskind explicitly discloses—and it would have been obvious to a POSITA—that directing users to these patches constitutes an offer to perform an action, namely installing the patch, which enables the user to obtain unrestricted Internet access after an infection and subsequent quarantine. This understanding is further supported by Roskind’s discussion of “monitoring a computer for infestation” and making “assertions about the cleanliness (e.g., infestation status)” of the computer after patch installation. For instance, Roskind

states that “in some embodiments, an operating system may respond with information associated with its patch level, wherein a sufficiently recent patch level may be interpreted as an assertion of cleanliness. If a computer asserts it is clean (1303) then monitoring is complete (1305) in this example” (Roskind, 14:19–26). Thus, a POSITA would have understood that the purpose of providing patch information for an infestation is to enable the user to access and install the patch to terminate the quarantine. *See also* Ex. 1006, 19:5–9, 25:20–23, 27:20–28:14, 24:7–12.

B. Dependent Method Claims

1. Claim 2: "The method according to claim 1, wherein the action requires the user to obtain and execute abnormal behavior scanning software from a server machine running at one of the one or more allowed network destination addresses."

103. In my opinion, Roskind discloses this limitation. Roskind discloses, or at minimum renders obvious, the method according to claim 1, wherein the action requires the user to obtain and execute abnormal behavior scanning software ("anti-contagion software") from a server machine running at one of the one or more allowed network destination addresses ("a site that provides anti-contagion software", "appropriate anti-contagion software distributor").

104. As I explained in [1c], Roskind teaches that a quarantined computer can be redirected to a quarantine notification page, which instructs the user to complete remediation steps before full network access is reinstated. For instance, Roskind

describes this page as “a web page that provides notification that the computer is quarantined, and/or provides links to remediation sites appropriate to the quarantine, such as a link to a site that provides anti-contagion software for removing a virus that the quarantined computer is believed to contain” (Roskind, 16:2–7).

105. Additionally, Roskind discloses that remediation requests may involve contacting “an appropriate anti-contagion software distributor, or...a security patch update provider,” with such requests being allowed to proceed while other traffic is blocked (*id.*, 14:53–61). Roskind also teaches that the quarantined client system may include “an agent associated with anti-contagion software installed on the client system 420” (*id.*, 6:63–7:23). From these disclosures, it is my opinion a POSITA would have understood that Roskind requires the quarantined computer’s user to retrieve anti-contagion software from an authorized remediation site and execute that software to remove the infection. Moreover, Roskind explicitly links remediation to a subsequent “assertion of cleanliness,” explaining that “the query for cleanliness (1302) may be responded to by anti-contagion software, such as antivirus software, with assertions about the currency of a scan...wherein a sufficiently updated software and/or scan may act as a cleanliness assertion” (Roskind, 14:12–19). Accordingly, Roskind discloses—and at minimum makes obvious—that the quarantined user must obtain and run anti-contagion software from an approved remediation server and perform a scan before the computer can assert its cleanliness

and regain unrestricted network access. *See also* Ex. 1006, 28:7–11, 25:11–18, 23:2–7.

2. Claim 3: "The method according to claim 1, further comprising: evaluating network traffic emanating from the client device after the client device has been scanned and abnormal behavior has been removed, mitigated or rendered inert."

106. In my opinion, Roskind discloses this limitation. Roskind discloses, or at minimum renders obvious, the method according to claim 1, further comprising: evaluating network traffic emanating from the client device after the client device has been scanned and abnormal behavior has been removed, mitigated or rendered inert.

107. Roskind discloses monitoring network traffic “for anomalous traffic” and explains that such monitoring “may be continuous.” For example, Roskind states that “a device near a computer, such as a firewall on a LAN or an ISP’s router, is used in some embodiments to monitor a computer for infestation (1201). Network traffic is monitored for anomalous traffic volume, port, or IP destination (1202). If an anomaly is detected (1203), then an apparent infestation is noted (1204).” A response to infestation may include quarantining the infected computer or network, as described in connection with Figures 14, 15, and 16. In some cases, remediation may also be attempted, such as inoculation, discussed in relation to Figure 17. Importantly, Roskind teaches that monitoring for anomalous traffic may be continuous, occurring before, during, and after infestation detection (Roskind,

13:10–53).

108. Further, Roskind explains that a “query for cleanliness (1302) may be responded to by anti-contagion software, such as antivirus software, with assertions about the currency of a scan, wherein a sufficiently updated software and/or scan may act as a cleanliness assertion,” or “wherein a sufficiently recent patch level may be interpreted as an assertion of cleanliness” (*id.*, 13:54–14:26). A person of ordinary skill in the art (POSITA) would have understood that continuous monitoring ensures that network traffic from the computer is evaluated throughout the infestation lifecycle—including before, during, and after identification and remediation via security patches or anti-contagion software. I also explained this above for limitations [1c], [2]. *See also* Ex. 1006, 21:19–22:20, 23:7–24:12.

3. Claim 4: "The method according to claim 1, further comprising: filtering the network traffic emanating from the client device to limit network packet flow by the client device. "

109. In my opinion, Roskind discloses this limitation. Roskind discloses, or at minimum renders obvious, the method according to claim 1, further comprising: filtering the network traffic emanating from the client device ("preventing unauthorized communications from being sent from the quarantined computer") to limit network packet flow by the client device. I incorporate my analysis for limitations [1b(a)], [1b(b)].

110. In my opinion at POSITA would have understood that quarantining an

infected computer to “prevent[] unauthorized communications from being sent” from the quarantined computer, as I discussed above in [1b(a)], discloses or at least renders obvious the filtering of network traffic originating from the client device—i.e., allowing authorized communications while blocking unauthorized ones—which inherently limits the network packet flow from the client device.

4. Claim 5: "The method according to claim 1, further comprising: routing the network traffic emanating from the client device to limit network packet traversal by the client device."

111. In my opinion, Roskind discloses this limitation. Roskind discloses, or at minimum renders obvious, the method according to claim 1, further comprising: routing the network traffic emanating from the client device to limit network packet traversal by the client device. I incorporate my analysis for limitations [1b(a)], [1c].

112. In my opinion, a POSITA would have understood that quarantining an infected computer to “prevent[] unauthorized communications from being sent” from the quarantined computer, as I explained above in [1b(a)], discloses or at least renders obvious the routing of network traffic originating from the client device exclusively to specifically authorized servers or destinations (e.g., “a site that provides anti-contagion software” or an “appropriate anti-contagion software distributor”). This approach inherently limits network packet traversal by the client device by blocking traffic to all non-approved systems.

5. Claim 6: "The method according to claim 1, wherein the plurality of quarantine control functions further comprises:

restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment."

113. In my opinion, Roskind discloses this limitation. Roskind discloses, or at minimum renders obvious, the method according to claim 1, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment.

114. As I explained in [1b(a)], Roskind discloses limiting network traffic from a quarantined computer to permit access only to designated remediation sites. It is my opinion a POSITA would have understood that such remediation sites—i.e., Internet-based web servers—are external to, and not subordinate to, the quarantined computer's first network segment.

6. Claim 7: "The method according to claim 1, further comprising: performing all of the plurality of quarantine control functions over the client device."

115. In my opinion, Roskind discloses this limitation. Roskind discloses, or at minimum renders obvious, the method according to claim 1, further comprising: performing all of the plurality of quarantine control functions over the client device.

116. As I explained above in [1b(a)] and [1b(b)], Roskind discloses restricting network traffic from a quarantined computer to a limited set of authorized

websites—such as “only allowing connections to a vendor’s server,” as described in [1b(a)]—and further restricting communications to those sites by permitting only specific network protocols. For example, “access to vendor sites is restricted by the quarantine to certain classes of traffic, such as HTTP requests,” as I explained in [1b(b)]. *See, e.g.,* Roskind, 11:15–56.

C. Independent Claims 8 and 15

117. I note that claims 8 and 15 are substantively aligned with claim 1, differing primarily in their preambles and introductory limitations. Claim 8 recites a "computer program product" configured to perform a method that is substantively the same as that of claim 1, while claim 15 recites a "network access gateway device"—also recited in claim 1—that is similarly programmed. Below, I address the preamble of claim 8 separately. The remaining limitations in claims 8 and 15 are unpatentable for the same reasons discussed with respect to claim 1 (or claim 8, as applicable), as detailed in the claim mapping provided below. I incorporate my analysis of claim 1 herein by reference.

1. Claim 8[pre]: "A computer program product comprising at least one non-transitory computer readable medium storing instructions translatable by at least one processor to perform:"

118. In my opinion, Roskind discloses this limitation. Roskind discloses, or at minimum renders obvious, a computer program product comprising at least one non-transitory computer readable medium storing instructions translatable by at least

one processor.

119. In my opinion, a POSITA would have understood that the method and system describe in claim 1 is implemented on a computer program product comprising at least one non-transitory computer readable medium storing instructions translatable by at least one processor. For example, Roskind discloses that its "invention can be implemented in numerous ways, including as...a computer readable medium such as a computer readable storage medium or a computer network wherein program instructions are sent over optical or electronic communication links. ...A component such as a processor or a memory described as being configured to perform a task includes both a general component that is temporarily configured to perform the task at a given time and a specific component that is manufactured to perform the task."); *E.g.*, Roskind, 2:47-60. Ex. 1006, 4:2-9.

2. 15[pre]: "A network access gateway device, comprising: at least one processor; and at least one non-transitory computer readable medium storing instructions translatable by the at least one processor to perform:"

120. In my opinion, Roskind discloses this limitation for the same reasons I set forth in 1[a] and 8[pre].

3. Remaining limitations of the Independent Claims

Claim 8	Claim 15	Claim 1
[8a]: "a plurality of quarantine control functions over a client device coupled to the network access gateway	[15c]: "a plurality of quarantine control functions over a client device coupled to the network access gateway	In my opinion, the limitations for claim 8 and claim 15 are disclosed, or at minimum rendered obvious for the

Claim 8	Claim 15	Claim 1
device, wherein the network access gateway device is between a local network and the Internet, wherein the client device is in a first network segment of the network, and wherein the plurality of quarantine control functions comprises:"	device, wherein the network access gateway device is between a local network and the Internet, wherein the client device is in a first network segment of the network, and wherein the plurality of quarantine control functions comprises:"	reasons I already set forth in [1a], [1b].
[8a(a)]: "restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment;	[15c(a)]: "restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment;"	In my opinion, the limitations for claim 8 and claim 15 are disclosed, or at minimum rendered obvious for the reasons I already set forth in [1b(a)].
[8a(b)]: "restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols; and"	[15c(b)]: "restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols; and"	In my opinion, the limitations for claim 8 and claim 15 are disclosed, or at minimum rendered obvious for the reasons I already set forth in [1b(b)].
[8b]: "rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to the implementation of one of the plurality of	[15d]: "rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to implementation of one of the plurality of	In my opinion, the limitations for claim 8 and claim 15 are disclosed, or at minimum rendered obvious for the reasons I already set forth in [1c].

Claim 8	Claim 15	Claim 1
quarantine control function of the client device."	quarantine control function of the client device."	

4. Dependent Claims 9-14 and 16-20

121. After analyzing the remaining dependent system claims I noticed that they are substantively the same as the corresponding method claims that I already addressed and are invalid for the reasons set forth above based upon the following mapping of claims. I therefore incorporate my analysis above herein.

Computer Program Product Dependent Claim	System Dependent Claim	Method Dependent Claim
9	16	2
10	17	3
11	18	4
12	19	5
13	20	6
14		7

XI. GROUNDS 3-4 - GLEICHAUF

A. Independent Claim 1

1. Claim 1[pre]: "A method of network traffic quarantine control, comprising:"

122. In my opinion, Gleichauf discloses this limitation. Gleichauf discloses, or at minimum renders obvious, a method of network traffic quarantine control.

123. Gleichauf explains that "a network management controller is provided that operates to immediately disable the communications capability of a rogue (or an infected computer) that contains an infective element." Gleichauf ¶ 06. This

action “prohibits the rogue from communicating to a next computer or to another destination, which may infect additional elements within the network.” *Id.* Gleichauf further emphasizes that this mechanism “allows for the quarantine of malicious traffic immediately after it is discovered within the network architecture.” *Id.*

124. Similarly, Gleichauf teaches that “network management controller 14 may then disable a communicating capability of infected computer 18 such that the infective element 12 may not be communicated to a next destination.” Gleichauf ¶ 19. The controller “may also implement other suitable actions...in order to sandbox, siderail, isolate, or otherwise disable infected computer 18 from communicating further.” *Id.* Gleichauf further explains that “[t]his community monitoring approach allows for the quarantine of malicious traffic immediately after it is discovered within the network architecture,” which is “particularly critical in network security systems where time is of the essence in containing damaging information...once a security breach has occurred.” Gleichauf ¶ 20.

2. Claim 1[a]: "at a network access gateway device between a local network and the Internet, selecting a client device in a first network segment of the network;"

125. In my opinion, Gleichauf discloses this limitation. Gleichauf discloses, or at minimum renders obvious, at a network access gateway device ("network management controller") between a local network ("internal network") and the Internet ("external network," "Internet"), selecting (in response to "a signal...that

identifies infected computer") a client device ("infected computer") in a first network segment of the network ("internal network").

126. Gleichauf explains that “FIG. 1 is a block diagram of a communication system 10 for detecting an infective element 12.... Communication system 10 includes a network management controller 14, multiple computers 16a–16d, an infected computer 18, an external network 22, and an internal network 24.” Gleichauf ¶ 17. The network management controller is described as being either “coupled to” or “inclusive of” a router that is “positioned at a gateway or at a communications interface.” Gleichauf ¶ 35. The router “may receive data packets from computers... and communicate those packets to [the] external network.” *Id.*

127. Gleichauf further explains that “a signal may be generated and transmitted... to network management controller [] such that a source associated with infective element [] is identified. This signal may include an address associated with infected computer 18.... Based on this signal, network management controller [] may then disable a communicating capability of [the] infected computer.” Gleichauf ¶ 19. Accordingly, upon identifying the infected source, the network management controller initiates quarantine control actions by selecting the infected computer for communication disablement.

3. Claim 1[b]: "at the network access gateway device, performing a plurality of quarantine control functions over the

client device, wherein the plurality of quarantine control functions comprises:"

128. In my opinion, Gleichauf discloses this limitation. Gleichauf discloses, or at minimum renders obvious, at the network access gateway device ("network management controller"), performing a plurality of quarantine control functions over the client device("the quarantine of malicious traffic"), wherein the plurality of quarantine control functions comprises [limitations [1b(a)]-[1b(b)]].

129. Gleichauf discloses that "a network management controller is provided that operates to immediately disable the communications capability of a rogue (or an infected computer) that contains an infective element.... This prohibits the rogue from communicating to a next computer or to another destination, which may infect additional elements within the network. The network management controller allows for the quarantine of malicious traffic immediately after it is discovered within the network architecture. This is important because time is a critical element in containing infective elements once they have penetrated the corresponding security system." Gleichauf ¶ 06. As further emphasized, "allow[ing] for the quarantine of malicious traffic immediately after it is discovered... is particularly critical in network security systems where time is of the essence in containing damaging information... once a security breach has occurred." Gleichauf ¶ 20. Gleichauf also notes that "Network management controller 14 may implement this and other appropriate remedial procedures in order to prohibit infected computer 18 from

communicating infective element 12 to a next destination. Network management controller 14 may also direct infected computer 18 to remediator website 30.” Gleichauf ¶ 32.

4. Claim 1[b(a)]: "restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment;"

130. In my opinion, Gleichauf discloses this limitation. Gleichauf discloses, or at minimum renders obvious, restricting all network traffic emanating from the client device ("disabl[ing] the communications capability of a rogue (or an infected computer)") to one or more network destination addresses that are not in or subordinate to the first network segment (permitting infected computer only "to communicate with the remediator website").

131. Gleichauf discloses that the network management controller “immediately disabl[es] the communications capability of a rogue (or an infected computer)... prohibit[ing] the rogue from communicating to a next computer or to another destination,” thereby blocking all traffic except as expressly permitted. Gleichauf ¶ 06; *see also id.* ¶ 19 (“network management controller 14 may then disable a communicating capability of infected computer 18 such that infective element 12 may not be communicated to a next destination. Network management controller 14 may also implement other suitable actions... in order to sandbox, siderail, isolate, or otherwise disable infected computer 18 from communicating

further”), ¶ 31 (“network management controller 14 may respond to the signal by employing sandboxing or siderailing techniques on the associated infected device or unit. In addition, network management controller 14 may position an infected device or unit on an island or suitably disable the infected device or unit”), ¶ 61 (“a communicating capability of infected computer 18 may be disabled.... Alternatively,...infected computer 18 may be disabled by employing sandboxing, constraining, isolating, or siderailing techniques.... Network management controller 14 may also execute any number of other actions in order to prohibit infected computer 18 from further communications.”).

132. In addition to disabling regular communications, Gleichauf further discloses that the network management controller may “direct [the computer containing an infected element] to a remediator website in order to comply with a network security enforcement protocol,” allowing the computer to “continue to communicate with the remediator website until it removes the infective element... at which time it may be permitted to resume communications with other network components.” Gleichauf ¶ 08; *see also id.* ¶ 52 (“Remediator website 30 is a security element designed to facilitate the removal of infective element 12 from infected computer 18... Infected computer 18 may be shunted or otherwise directed to remediator website 30 until the proper software or configurations are downloaded or until infective element 12 is removed from infected computer 18.”). Thus, Gleichauf

discloses restricting all traffic emanating from the client device solely to the remediator website.

133. Additionally, Gleichauf describes the remediator's website as being "coupled to internal network 24 and infected computer 18" (Gleichauf ¶ 52]), but does not necessarily require that the remediator's website reside within the internal network itself. Gleichauf defines the "internal network" broadly as any network architecture, including a LAN, MAN, WAN, or other system facilitating communications (Gleichauf ¶ 50). To the extent Patent Owner argues that "coupled to internal network 24 and infected computer 18" means the remediator's website must be within or subordinate to the same network as the infected computer, it is my opinion that a POSITA would have at minimum found it obvious that the remediator's website could be located on an external network, such as the Internet. In my opinion, placement of the remediator's website on either an internal or external network is a straightforward design choice well known and obvious to a POSITA.

5. Claim 1b(b): "restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols;"

134. In my opinion, Gleichauf discloses this limitation. Gleichauf discloses, or at minimum renders obvious, restricting all network traffic emanating from the client device ("disabl[ing] the communications capability of a rogue (or an infected

computer)") to an allowed network destination address ("remediator websites") to selected one or more network protocols ("TCP/IP").

135. As I discussed in [1b(a)], Gleichauf discloses disabling all communications from an infected computer except for communications with a designated "remediator website." For example, Gleichauf explains that "[a] computer containing an infective element may be directed to a remediator website in order to comply with a network security enforcement protocol" (Gleichauf, ¶ 8), and that the "network management controller 14 may implement...appropriate remedial procedures in order to prohibit infected computer 18 from communicating infective element 12 to a next destination. Network management controller 14 may also direct infected computer 18 to remediator website 30. Infected computer 18 may then communicate with remediator website 30 until infective element 12 is removed or until infected computer 18 is otherwise brought in compliance with suitable networking security protocols" (Gleichauf ¶ 32).

136. Gleichauf further discloses that communications on both the internal and external networks are implemented using the "TCP/IP communication language protocol." Gleichauf ¶¶ 49, 50. Gleichauf also describes a "policies node" that "includes protocols that dictate what may be accessed and run by elements within the communication system," including policies on "any other suitable network enhancement or communications feature." *Id.*, ¶ 57. The network management

controller may use these policies “in order to disable one or more of those policies or services being provided to infected [computer] 18 until it properly complies with the requisite security parameters.” *Id.*, ¶ 58; *see also id.*, ¶ 61 (network management controller 14 may access policies node 38 to restrict services offered to infected computer 18). In my opinion, a POSITA would have understood, or at minimum found obvious, that restricting policies in this manner—i.e., disabling one or more policies or services until compliance—would include limiting the use of network protocols other than TCP/IP that are needed to access the remediator’s website. This ensures that only authorized traffic—TCP/IP traffic to the remediation website—is allowed, while all other potentially harmful traffic is blocked.

6. Claim 1[c]: "and rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to implementation of one of the plurality of quarantine control function of the client device."

137. In my opinion, Gleichauf discloses this limitation. Gleichauf discloses, or at minimum renders obvious, rendering a web page to display on the client device from the network access gateway device ("signal", "broadcast signal", "alert signal"), wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet (communications blocked "until the proper software or configurations are downloaded or until infective element [] is removed from infected computer")

responsive to implementation of one of the plurality of quarantine control function of the client device.

138. Gleichauf discloses a “web browser” on the infected computer that can be used to “view pages.” Gleichauf, ¶ 27. Upon detection of an infection, a “communication protocol shim” may generate a signal that is transmitted to the network management controller and other computers, thereby signaling the presence of the infective element on the infected computer. *Id.*, ¶ 44 (“Communication protocol shim 42 may be configured such that once infected element 12 is identified, a signal is generated and sent to network management controller 14.... Communication protocol shim 42 may signal the presence of infective element 12 at infected computer 18 in any number of ways...”). This includes sending a direct signal to infected computer 18 indicating the presence of the infective element within its internal structure, which in response may communicate with the remediator website or alternatively perform some cleaning or security check. *Id.*, ¶ 44; see also ¶ 45. Additionally, Gleichauf discloses that the network management controller may broadcast an alert signal to components within the communication system. Gleichauf, ¶ 61; see also ¶ 60. This alert signal may include information such as the type of damaging element present in the network or remedial measures to be taken. *Id.*, ¶ 32; see also ¶ 47 (“broadcast signal may include the type of damaging element present...and further provide remedial measures to be taken if the damaging element

is subsequently encountered”), ¶ 48 (“the signal may include information for remedial measures for coping with or for combating the damaging element...[or] include any other suitable information that offers some guidance in handling the presence or harmful effects of infective element”), ¶ 60 (“signal may include...the remedial measures to be taken when encountering infective element 12, or any other suitable information relating to the presence of infective element 12. The signal may be communicated directly to infected computer 18...”).

139. It is my opinion that a POSITA would have understood, or at minimum found it obvious, that the network management controller could, like the communication protocol shim, broadcast an alert “signal directly to infected computer” identifying the “damaging element...[and] remedial measures” for addressing it. Gleichauf, ¶¶ 32, 47-48. Further, because the “signal” includes information such as “remedial measures for coping with or for combating the damaging element,” a POSITA would have found it an obvious design choice to implement the signal in a user-friendly format—such as a web page sent from the network management controller to the infected computer, informing the user of the infection and remediation steps, including visiting a remediation website. By delivering a web page from the controller to the infected computer, the controller could efficiently notify the user why communications are blocked and instruct how to remediate the issue to restore regular network access—such as by installing

software from a remediator website that facilitates removal of the infective element, as discussed in [2]. This implementation would have been straightforward and would have yielded expected results at the time. Moreover, the fact that the “alert” is also broadcast to all other devices on the network further suggests—and at minimum renders obvious—that the web page would be graphically rendered at the server and transmitted in an accessible format to ensure prompt and clear communication of the alert information.

B. Dependent Method Claims

1. Claim 2: "The method according to claim 1, wherein the action requires the user to obtain and execute abnormal behavior scanning software from a server machine running at one of the one or more allowed network destination addresses."

140. In my opinion, Gleichauf discloses this limitation. Gleichauf discloses, or at minimum renders obvious, the method according to claim 1, wherein the action requires the user to obtain and execute abnormal behavior scanning software ("hardware, software, or any other object or element that combats or that facilitates the removal of infective element", "virus detection element") from a server machine running at one of the one or more allowed network destination addresses ("remediator website").

141. I incorporate my analysis from 1[c] above. In addition, it is my opinion that a POSITA would have understood that Gleichauf’s disclosure of quarantining an infected computer and blocking all communications other than those to a

remediator website “until the proper software or configurations are downloaded” (Gleichauf, ¶ 52) discloses, and at minimum renders obvious, the requirement that the user download and execute virus scanning software, or similar remediation tools, in order to restore normal communications. *See* Gleichauf, ¶ 32 (allowing only “communicat[ions] with remediator website 30 until infective element 12 is removed or until infected computer 18 is otherwise brought in compliance”).

142. Further, in my opinion, a POSITA would have understood that Gleichauf discloses, or at minimum renders obvious, that the remediator website provides an updated “virus detection element” as an example of software “that combats or that facilitates the removal of infective element.” Specifically, Gleichauf discloses that the remediator website, which includes “software...that combats or that facilitates the removal of infective element,” will “evaluate infected computer 18 and determine that it is in proper security compliance,” thereby disclosing, or at minimum rendering obvious, the scanning of the infected computer for abnormalities. Gleichauf, ¶ 52.

143. Likewise, Gleichauf describes a “virus detection element” as “any hardware, software, or elements operable to detect a damaging element, such as infective element 12, present in communication system 10.” Virus detection element 40 may also be a desktop firewall product, such as those produced by Symantec Inc., Network Associates, or Computer Associates, that perform security screening to

ensure the corresponding element is free of harmful elements. Virus detection element 40 may further be capable of identifying particular types of damaging elements, such as a Trojan, worm, or virus. Gleichauf, ¶ 42. Further, Gleichauf discloses that computers without a “virus detection element” are “not in compliance with any security protocol.” Gleichauf, ¶ 41. In my opinion, a POSITA thus would have understood that bringing such a computer into compliance (i.e., an infected computer without a virus detection element) would require downloading and executing a valid virus detection element on the infected computer.

2. Claim 3: "The method according to claim 1, further comprising: evaluating network traffic emanating from the client device after the client device has been scanned and abnormal behavior has been removed, mitigated or rendered inert."

144. In my opinion, Gleichauf discloses this limitation. Gleichauf discloses, or at minimum renders obvious, the method according to claim 1, further comprising: evaluating network traffic ("routines or programs that execute pattern matching, looking for specific or systematic traffic behavior") emanating from the client device after the client device has been scanned and abnormal behavior has been removed, mitigated or rendered inert.

145. Gleichauf discloses using the “virus detection element” to “execute pattern matching, looking for specific or systematic traffic behavior.” Gleichauf, ¶ 42. A POSITA would have understood that Gleichauf therefore discloses, or at minimum renders obvious, performing such traffic pattern matching on

communications from all computers—including the infected computer—before, during, and after an infection is identified and mitigated. I also incorporate my analysis from [1c], [2], above.

3. Claim 4: "The method according to claim 1, further comprising: filtering the network traffic emanating from the client device to limit network packet flow by the client device. "

146. In my opinion, Gleichauf discloses this limitation. Gleichauf discloses, or at minimum renders obvious, the method according to claim 1, further comprising: filtering the network traffic emanating from the client device ("disabl[ing] the communications capability of a rogue (or an infected computer)") to limit network packet flow by the client device.

147. I incorporate my analysis from [1b(a)], [1b(b)] above. In my opinion, a POSITA would have understood that quarantining an infected computer to "disable the communications capability of a rogue (or an infected computer)," as discussed above in [1b(a)], discloses or at minimum renders obvious filtering the network traffic emanating from the client device—i.e., allowing authorized communications while preventing unauthorized ones—which would inherently limit the network packet flow generated by the client device.

4. Claim 5: "The method according to claim 1, further comprising: routing the network traffic emanating from the client device to limit network packet traversal by the client device."

148. In my opinion, Gleichauf discloses this limitation. Gleichauf discloses,

or at minimum renders obvious, the method according to claim 1, further comprising: routing the network traffic emanating from the client device ("shunt[] or otherwise direct[traffic] to remediator website") to limit network packet traversal by the client device.

149. I incorporate my analysis from [1b(a)], [1b(b)] above. In my opinion, a POSITA would have understood that quarantining an infected computer such that it is "shunted or otherwise directed to remediator website 30" until the problem is resolved, as discussed above in [1b(a)], discloses or at minimum renders obvious routing the network traffic emanating from the client device exclusively to specifically allowed servers or sites (e.g., the "remediator website"), thereby limiting network packet traversal by the client device by blocking traffic to any non-approved computers.

5. Claim 6: "The method according to claim 1, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first network segment."

150. In my opinion, Gleichauf discloses this limitation. Gleichauf discloses, or at minimum renders obvious, the method according to claim 1, wherein the plurality of quarantine control functions further comprises: restricting all network traffic emanating from the client device to one or more network destination addresses in one or more network segments that are not in or subordinate to the first

network segment.

151. I incorporate my analysis from [1b(a)] above. As discussed I in [1b(a)], Gleichauf discloses limiting traffic from the quarantined computer to allow access only to remediation websites. In my opinion, a POSITA would have understood that such remediation sites—i.e., Internet websites—are not located within the first network segment.

6. Claim 7: "The method according to claim 1, further comprising: performing all of the plurality of quarantine control functions over the client device."

152. In my opinion, Gleichauf discloses this limitation. Gleichauf discloses, or at minimum renders obvious, the method according to claim 1, further comprising: performing all of the plurality of quarantine control functions over the client device.

153. As I discussed above in [1b(a)] and [1b(b)], Gleichauf discloses restricting network traffic from the quarantined computer to only certain allowed websites (e.g., only the "remediator website" as set forth in [1b(a)]) and further restricting communications to those sites using only certain protocols (e.g., limiting services but allowing TCP/IP connections to the remediation website) as I explained in [1b(b)]. *See, e.g.*, Roskind, 11:15-56.

C. Independent Claims 8 and 15

154. I note that claims 8 and 15 are substantively aligned with claim 1,

differing primarily in their preambles and introductory limitations. Claim 8 recites a "computer program product" configured to perform a method that is substantively the same as that of claim 1, while claim 15 recites a "network access gateway device"—also recited in claim 1—that is similarly programmed. Below, I address the preamble of claims 8 separately. The remaining limitations in claims 8 and 15 are unpatentable for the same reasons discussed with respect to claim 1 (or claim 8, as applicable), as detailed in the claim mapping provided below. I incorporate my analysis of claim 1 herein by reference.

1. Claim 8[pre]: "A computer program product comprising at least one non-transitory computer readable medium storing instructions translatable by at least one processor to perform:"

155. In my opinion, Gleichauf discloses this limitation. Gleichauf discloses, or at minimum renders obvious, a computer program product comprising at least one non-transitory computer readable medium storing instructions translatable by at least one processor.

156. I incorporate my analysis from claim 1 above herein. Gleichauf further discloses a "network management controller" that "may include any hardware, software, object, or elements" configured to perform the disclosed methods. Gleichauf, ¶ 30. To the extent not explicitly stated, it is my opinion that a POSITA would have understood that computer "hardware" and "software" programmed to carry out the invention necessarily include, and at minimum render obvious, some

form of a processor and a non-transitory computer-readable medium storing instructions to implement the disclosed functionality.

2. 15[pre]: "A network access gateway device, comprising: at least one processor; and at least one non-transitory computer readable medium storing instructions translatable by the at least one processor to perform:"

157. In my opinion, Gleichauf discloses this limitation for the same reasons I set forth in 1[a] and 8[pre].

3. Remaining limitations of the Independent Claims

Claim 8	Claim 15	Claim 1
[8a]: "a plurality of quarantine control functions over a client device coupled to the network access gateway device, wherein the network access gateway device is between a local network and the Internet, wherein the client device is in a first network segment of the network, and wherein the plurality of quarantine control functions comprises:"	[15c]: "a plurality of quarantine control functions over a client device coupled to the network access gateway device, wherein the network access gateway device is between a local network and the Internet, wherein the client device is in a first network segment of the network, and wherein the plurality of quarantine control functions comprises:"	In my opinion, the limitations for claim 8 and claim 15 are disclosed, or at minimum rendered obvious for the reasons I already set forth in [1a], [1b].
[8a(a)]: "restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment;	[15c(a)]: "restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or subordinate to the first network segment;"	In my opinion, the limitations for claim 8 and claim 15 are disclosed, or at minimum rendered obvious for the reasons I already set forth in [1b(a)].

Claim 8	Claim 15	Claim 1
[8a(b)]: "restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols; and"	[15c(b)]: "restricting all network traffic emanating from the client device to an allowed network destination address to selected one or more network protocols; and"	In my opinion, the limitations for claim 8 and claim 15 are disclosed, or at minimum rendered obvious for the reasons I already set forth in [1b(b)].
[8b]: "rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to the implementation of one of the plurality of quarantine control function of the client device."	[15d]: "rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to implementation of one of the plurality of quarantine control function of the client device."	In my opinion, the limitations for claim 8 and claim 15 are disclosed, or at minimum rendered obvious for the reasons I already set forth in [1c].

D. Dependent Claims 9-14 and 16-20

158. After analyzing the remaining dependent system claims I noticed that they are substantively the same as the corresponding method claims that I already addressed and are invalid for the reasons set forth above based upon the following mapping of claims. I therefore incorporate my analysis above herein.

Computer Program Product Dependent Claim	System Dependent Claim	Method Dependent Claim
9	16	2
10	17	3

11	18	4
12	19	5
13	20	6
14		7

XII. GROUNDS 5 AND 6 – GROUNDS 1-4 IN VIEW OF SHORT

159. As I discussed above in Grounds 1 and 2 (Roskind) and Grounds 3 and 4 (Gleichauf), Roskind and Gleichauf each disclose, and at minimum render obvious, all the limitations of Challenged Claims 1–20. Regarding Claim 1’s limitation of “rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet responsive to implementation of one of the plurality of quarantine control functions of the client device” (element [1c]), Roskind discloses a “browser” on the client computer that is redirected to a “quarantine server [] configured to provide a notice and other information and/or instructions to a user of the quarantined host.” A POSITA would have understood that browsers are used to render web pages. Roskind further discloses that the quarantine server “resides on the router...and/or gateway.” Roskind, 12:11–13; see also my analysis for Grounds 1 and 2. To the extent it is argued that Roskind is not entitled to its 9/27/2004 priority date for this disclosure, Short discloses such a server residing on a gateway device. *E.g.*, Short, 4:13–21.

160. Likewise, Gleichauf discloses transmitting a “signal” containing

detailed information about the presence of, and how to remedy, an infection, and a POSITA would have found it obvious to implement this signal as a web page transmitted from the network management controller to the infected computer. See my analysis for Grounds 3 and 4. To the extent further disclosure is required regarding such a web page transmitted from a server residing on a router or gateway, a POSITA would have found it obvious to implement these teachings as disclosed by Short.

161. Short discloses a gateway device that “serves as an interface connecting [a] user to a number of networks or other online services,” such as the Internet or an enterprise network. Short, 2:5-9. This gateway enables Internet Service Providers (ISPs) and enterprise network providers (e.g., hotels) to offer users simple and transparent access to their networks and other online services. Short, 2:45-53. To facilitate this, providers may “redirect users to portal pages that [they]...wish the user to access or view,” including login pages where users enter credentials to be authenticated and authorized. Short, 3:9-12. Importantly, Short discloses that these portal pages can be maintained on a web server local to the gateway device. Short, 5:32-34; see also 4:13-21 (describing establishing a login page on a local web server prior to redirecting the user) and 4:54-55 (“login page is maintained local to the gateway device”). Hosting the web server locally allows the redirection to be “efficient and fast.” Short, 9:5-15.

162. Short further teaches that this redirection can be limited to specific traffic types, such as web pages only, excluding emails, FTP, or other traffic. Short, 9:26-48. The portal page can contain any information, including personalized content and offers for services from the network provider, such as offers related to network connectivity. Short, 8:20-30; 10:5-19. Users are directed to a login page where they must input information that the gateway uses to authorize access to the destination network, which can be an Internet destination. Short, 4:22-25; 4:54-59.

163. Thus, Short discloses “rendering a web page to display on the client device from the network access gateway device, wherein the web page contains an offer for a user of the client device to perform an action in order to obtain unrestricted access to the Internet.”

164. Furthermore, it is my opinion that a POSITA would have been motivated to apply Short’s teachings to the quarantine control systems disclosed by Roskind and Gleichauf. Like Roskind and Gleichauf, Short addresses controlling access to networks and is reasonably pertinent to the same problems alleged in the ’710 patent, such as implementing a gateway to control unauthorized computer access. See, e.g., Roskind, 3:10-23 (disclosing “[a]nalyzing routing information to identify and intercept unauthorized...communications”); Gleichauf, ¶ 6 (teaching quarantine of malicious traffic immediately upon discovery within the network); Short, 4:17-20 (describing acceptance of user information by the gateway device to

authorize network access). Roskind and Gleichauf already teach quarantining communications to restrict unauthorized use of protected network resources, including redirection of quarantined computers to a quarantine server or “remediator website.” See my analysis for Grounds 1 and 2 at [1b], [1b(a)], [1b(b)], [1c] and my analysis for Grounds 3 and 4 at limitations [1b], [1b(a)], [1b(b)], [1c].

165. Accordingly, it is my opinion that a POSITA would have been motivated to incorporate well-understood implementation details from Short—such as hosting the quarantine server local to the gateway for efficient, fast redirection, and providing user offers to obtain or regain network access, including Internet access—into Roskind and Gleichauf’s quarantine control systems. It is my opinion that a POSITA would have readily recognized that modifying these existing systems, which already redirect quarantined clients based on quarantine control functions, with Short’s teachings would have yielded a method that renders a web page on the client device from the network access gateway, wherein the web page offers the user an action to gain unrestricted Internet access responsive to implementation of one of the quarantine control functions—thus rendering claims 1–20 obvious. And, in my opinion, POSITA would have had a reasonable expectation of success in making this modification, as locally-hosted web servers for such purposes were well understood and routinely used in the field.

XIII. SECONDARY CONSIDERATIONS OF NON-OBVIOUSNESS

166. Neither the applicant nor the Examiner identified any secondary considerations that favored a finding of non-obviousness during prosecution of the application that issued as the '710 Patent. *See generally* EX1002. Further, I am unaware of any secondary considerations that tend to show non-obviousness of the Challenged Claims. To the extent that such secondary considerations become available to me in the course of this proceeding, I reserve the right to address them in a supplemental declaration.

167. I declare under penalty of perjury that the foregoing is true and correct.
Executed this 13th day of October, 2025 in Louisville, Colorado.

A handwritten signature in black ink, appearing to be 'J. B. J.', is written above a horizontal line.

Appendix A

John R. Black, Jr.

Department of Computer Science
430 UCB
University of Colorado
Boulder, CO 80309-0430 USA

office: +1 303 492-0573
FAX: +1 303 492-2844
secretary: +1 303 492-7514

Email: jrblack@cs.colorado.edu
WWW: <http://www.cs.colorado.edu/~jrblack/>

Position	Assoc. Prof. Computer Science, University of Colorado at Boulder	<i>7/08–present</i>
Research	Cryptography, Network Security, Computer Security.	
Past Employment	SecureSet LLC Vice President of Education	<i>9/15–7/18</i>
	University of Colorado at Boulder Assistant Professor of Computer Science.	<i>7/02–7/08</i>
	University of Nevada, Reno Assistant Professor of Computer Science.	<i>7/00–6/02</i>
	University of California, Davis Research Assistant	<i>7/97–7/00</i>
	University of California, Davis Teaching Assistant	<i>8/95–6/97</i>
	Ingres Corporation Senior Member of Technical Staff	<i>6/88–4/94</i>
Education	University of California, Davis Ph.D. in Computer Science. Thesis: Message Authentication Codes. Advisor: Phillip Rogaway.	<i>9/95–9/00</i>
	California State University at Hayward B.S. in Computer Science and Mathematics, 1988. Honors: Summa Cum Laude	<i>9/84–6/88</i>
Awards	NSF CAREER Award, 2002 Chancellor's Teaching Fellowship, UC Davis, 1998 Outstanding Teaching Assistant, UC Davis, 1998 Outstanding Teaching Assistant, UC Davis, 1997 A Check for \$2.56 from Don Knuth, 1996	

Journal Publications

1. P. Rogaway, M. Bellare and J. Black, “OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption.” *ACM Transactions on Information and System Security (TISSEC)*, Volume 6, Issue 3, pp. 365–403, August, 2003.
2. J. Black, and P. Rogaway, “CBC MACs for Arbitrary Length Messages: The Three-Key Constructions.” *Journal of Cryptology*, Volume 18, Number 2, pp. 111–132, Spring, 2005.
3. J. Black, “The Impossibility of Technology-Based DRM and a Modest Suggestion.” *Journal of Telecommunications and High-Technology Law —JTHTL*, Volume 3, Number 2, pp. 387–396, Spring, 2005.
4. J. Black, M. Cochran and R. Gardner, “An Analysis of the Internet Chess Club.” *IEEE Security and Privacy*, Volume 4, Number 1, pp. 46–52, January, 2006.
5. J. Black, M. Cochran and T. Shrimpton, “On the Impossibility of Highly-Efficient Blockcipher-Based Hash Functions.” *Journal of Cryptology*, Volume 22, Number 3, pp. 311–329, Fall, 2009.
6. J. Black, P. Rogaway, T. Shrimpton, and M. Stam “An Analysis of the Blockcipher-Based Hash Functions from PGV.” *Journal of Cryptology*, Volume 23, Number 4, pp. 519–545, Fall, 2010.
7. C. Wilks, M. Cline, E. Weiler, M. Diehkans, B. Craft, C. Martin, D. Murphy, H. Pierce, J. Black, D. Nelson, B. Litzinger, T. Hatton, L. Maltbie, M. Ainsworth, P. Allen, L. Rosewood, E. Mitchell, B. Smith, J. Warner, J. Groboske, H. Telc, D. Wilson, B. Sanford, H. Schmidt, D. Haussler, D. Maltbie “The Cancer Genomics Hub (CGHub): overcoming cancer through the power of torrential data.” *Database*, Volume 2014, doi: 10.1093/database/bau093.

Book Chapters

1. J. Black, “Cryptography.” Invited article for the Encyclopedia of Life Support Systems under the auspices of UNESCO. See <http://www.eolss.net>. 14 pages, March, 2004.
2. J. Black, “Authenticated Encryption.” Invited article for the *Encyclopedia of Cryptography and Security*, Springer-Verlag. 12 pages. August, 2005.

**Conference
Publications
(Refereed)**

1. J. Black, C. Martel, and H. Qi, “Graph and Hashing Algorithms for Modern Architectures: Design and Performance.” *Workshop on Algorithm Engineering — WAE ’98*, Saarbrücken, Germany. Second Workshop on Algorithm Engineering, proceedings, pp. 37–48. Full version of this paper available at theory.cs.ucdavis.edu.
2. J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, “UMAC: Fast and Secure Message Authentication.” *Advances in Cryptology — CRYPTO ’99*, Lecture Notes in Computer Science, Vol. 1666, Springer-Verlag, pp. 216–233, 1999. Full version and updated version of this paper available at www.cs.ucdavis.edu/~rogaway/umac.
3. J. Black and P. Rogaway, “CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions.” *Advances in Cryptology — CRYPTO 2000*, Lecture Notes in Computer Science, Vol. 1880, Springer-Verlag, pp. 197–215, 2000.
4. P. Rogaway, M. Bellare, J. Black and T. Krovetz, “OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption.” *Eighth ACM Conference on Computer and Communications Security (CCS-8)*, ACM Press, pp. 196–205, 2001.
5. J. Black and P. Rogaway, “Enciphering Finite Sets of Arbitrary Size.” *RSA Data Security Conference, Cryptographer’s Track (RSA-CT)*, Lecture Notes in Computer Science, Vol. 2271, Springer-Verlag, pp. 114–130, 2002.
6. J. Black and P. Rogaway, “A Block-Cipher Mode of Operation for Parallelizable Message Authentication.” *Advances in Cryptology — EUROCRYPT 2002*, Lecture Notes in Computer Science, Vol. 2332, Springer-Verlag, pp. 384–397, 2002.
7. J. Black and H. Urtubia, “Side-Channel Attacks on Symmetric Encryption Schemes: The Case for Authenticated Encryption.” *USENIX Security Symposium — Security ’02*. 10 pages, 2002.
8. J. Black, P. Rogaway, and T. Shrimpton, “Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV.” *Advances in Cryptology — CRYPTO 2002*, Lecture Notes in Computer Science, Vol. 2442. 16 pages, 2002.
9. J. Black, P. Rogaway, and T. Shrimpton, “Encryption Scheme Security in the Presence of Key-Dependent Messages.” *Selected Areas in Cryptography — SAC 2002*, Lecture Notes in Computer Science, Vol. 2595, 14 pages, 2002.
10. R. Motwani, J. Breidenbach and J. Black, “Collocated Dataglyphs for Large Message Storage and Retrieval.” *Security, Steganography, and Watermarking of Multimedia Contents VI*, Society for Imaging Science and Technology (I&ST) jointly with International Society for Optical Engineering (SPIE), Vol. 5306, 19 pages, 2004.
11. J. Black, M. Cochran and T. Shrimpton, “On the Impossibility of Highly-Efficient Blockcipher-Based Hash Functions.” *Advances in Cryptology — EUROCRYPT 2005*, Lecture Notes in Computer Science, Vol. 3494, Springer-Verlag, pp. 526–541, 2005.
12. J. Black, M. Cochran and R. Gardner, “Lessons Learned: A Security Analysis of the Internet Chess Club.”, *Annual Computer Security Applications Conference — ACSAC 2005*, Tucson AZ, USA, pp. 220–228, 2005.
13. J. Black and M. Cochran and T. Highland, “A Study of the MD5 Attacks: Insights and Improvements”, *Fast Software Encryption — FSE 2006*, Lecture Notes in Computer Science, Vol. 4047, Springer-Verlag, pp. 262–277, 2006.

**Conference
Publications
(cont.)**

14. J. Black, “The Ideal-Cipher Model, Revisited: An Uninstantiable Blockcipher-Based Hash Function.”, *Fast Software Encryption — FSE 2006*, Lecture Notes in Computer Science, Vol. 4047, Springer-Verlag, pp. 328–340, 2006.
15. J. Black, “Compare-by-Hash: A Reasoned Analysis”, *USENIX Annual Technical Conference — USENIX 2006*, 8 pages, 2006.
16. J. Black and M. Cochran, “MAC Reforgeability”, *Fast Software Encryption — FSE 2009*, Lecture Notes in Computer Science, Vol. 5665, Springer-Verlag, pp. 345–362, 2009.
17. J.H. Huang, J. Black, and S. Mishra, “Security and Privacy in a Sensor-Based Search and Rescue System,” *1st ICST/CREATE-NET International Conference on Ad Hoc Networks — ADHOCNETS 2009*, Vol. 28, Springer.
18. A. Sayler, D. Grunwald, J. Black, E. White, M. Monaco, “Supporting CS education via virtualization and packages: tools for successfully accommodating “bring-your-own-device” at scale,” *SIGCSE 2014*, pp. 313-318, 2014.

**Workshop
Publications
(Non-
Refereed)**

1. J. Black and P. Rogaway, “A Suggestion for Handling Arbitrary-Length Messages with the CBC MAC.” *NIST Symmetric Key Block Cipher Modes of Operation Workshop—2000*, 4 pages, Sep 2000.
2. J. Black and P. Rogaway, “OCB: Proposal to NIST.” *2nd NIST Symmetric Key Block Cipher Modes of Operation Workshop—2001*, 36 pages, Aug 2001.
3. J. Black and P. Rogaway, “PMAC: Proposal to NIST.” *2nd NIST Symmetric Key Block Cipher Modes of Operation Workshop—2001*, 27 pages, Aug 2001.

Selected Talks

1. Data Structures for Fast Graph Algorithms. Presented at the 1997 UC Davis Workshop on Computing, Davis, USA, October 1997. (See Conference Publication #1.)
2. UMAC: Fast and Secure Message Authentication. Presented at CRYPTO '99, Santa Barbara, USA, August 1999. (See Conference Publication #2)
3. CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions. Presented at CRYPTO 2000, Santa Barbara, USA, August 2000. (See Conference Publication #3)
4. A Suggestion for Handling Arbitrary-Length Messages with the CBC MAC. Presented at NIST Symmetric Key Block Cipher Modes of Operation Workshop—2000, October, 2000; also presented at the 2nd NIST Modes Workshop in Santa Barbara, USA, August 2001.
5. Enciphering Finite Sets of Arbitrary Size. Presented at RSA-CT '02, San Jose, USA, February 2002. (See Conference Publication #5)
6. A Block-Cipher Mode of Operation for Parallelizable Message Authentication. Presented at EUROCRYPT 2002, Amsterdam, The Netherlands, May 2002. (See Conference Publication #6)
7. Side-Channel Attacks on Symmetric Encryption Schemes. Presented at USENIX Security 2002, San Francisco, USA, August 2002. (See Conference Publication #7)
8. Practical Cryptography and Autonomic Web Computing. Invited talk at the 47th meeting of the IFIP Working Group 10.4. Rincon, Puerto Rico, January 2005.
9. On the Impossibility of Highly-Efficient Blockcipher-Based Hash Functions. Presented at EUROCRYPT 2005, Aarhus, Denmark, May 2005. (See Conference Publication #11)
10. The Ideal-Cipher Model, Revisited: An Uninstantiable Blockcipher-Based Hash Function. Presented at FSE 2006, Graz, Austria, March 2006. (See Conference Publication #14)
11. Compare-by-Hash: A Reasoned Analysis. Presented at USENIX Technical Conference 2007, Boston, MA, June 2006. (See Conference Publication #15)

Patents

1. T. McSheery, J. Black, S. Nollet, J. Johnson, and V. Jivan. Distributed-Processing Motion Tracking System for Tracking Individually Modulated Light Points. US Patent 6,324,296 B1. November 2001.

Funding

1. NCHIA E-Team Grant. “Entrepreneurship for Undergraduates.” PI: John Black. Period: 2000-2001. Amount: \$6,000.
2. University of Nevada Junior Faculty Research Grant. “Fast, Provably-Secure Cryptography.” PI: John Black. Period: 2001-2002. Amount: \$10,000.
3. NSF CAREER Award. “Highly-Optimized Provably-Secure Cryptography.” PI: John Black. Period: 2002-2007. Amount: \$469,925.
4. NSF NeTS Grant. “NeTS ProWIN: Topology And Routing With Steerable Antennas.” PI: Dirk Grunwald. Co-PIs: John Black, Douglas Sicker. Period: 2005–2008. Amount: \$745,215.
5. NSF Cybertrust Grant. “Cryptography for Constrained Environments.” PI: John Black. Period: 2005–2008. Amount: \$294,887.

Teaching History

ECS 122A — Design and Analysis of Algorithms (UC Davis). Co-taught once with Professor Rogaway; subsequently taught the course independently.

CMPSC 290G — Intro to Cryptoanalysis (UCSB).

CS 365 — Discrete Mathematics (UNR).

CS 425 — Software Engineering (UNR).

CS 426 — Senior Projects (UNR). Supervised 11 group projects in topics ranging from fingerprint recognition to audio editing to GUI design.

CS 432 — Computer Networks (UNR). Introduction to low-level networking concepts with an emphasis on network security.

CS 665 — Graduate Analysis of Algorithms (UNR). A typical algorithms course with emphasis on complexity theory.

CS 709 — Modern Cryptography (UNR). A graduate course introducing cryptography and visiting some of the research front.

CS 791G — Computer Network Security (UNR). A seminar course covering various topics related to network security.

CSCI 2270 — Data Structures (CU); Program design, Object orientation, Java, Linked lists, Arrays, Stacks and Queues, Hash tables, Trees, Balanced Binary Trees, Multi-core programming.

CSCI 3104 — Algorithms (CU); Divide-and-conquer, Greedy, Graph Algorithms, NP-Completeness, Quantum Algorithms.

CSCI 3753 — Operating Systems (CU); Scheduling, Virtual Memory, Filesystems, Multi-core systems, Pthreads, Kernel data structures, virtualization, Security.

CSCI 4830 — Network Security (CU); a new course developed to introduce basics of cryptography and network security. Covers SSL, PKI, DDOS attacks, wireless security, buffer overruns, and more.

CSCI 4900 — Solving Puzzles with Computers (CU); a one-unit undergraduate course describing some hard combinatorial puzzles and how computers can be used to attack them.

CSCI 5413 — Ethical Hacking (CU); Network security, nmap, netcat, Kali Linux, Buffer overruns, Format string vulnerabilities, Race Conditions, Web Security, SQL Injections, XSS, CSRF, Wireless.

CSCI 6268 — Foundations of Computer and Network Security (CU); an introductory course covering basic cryptography, cryptographic protocols, attacks, and principles, as well as core network security attack and defense.

CSCI 7000 — Cryptography Seminar (CU); A graduate course introducing basic cryptographic definitions and then making some forays to the research front.

CSCI 7000 — Cryptanalysis Seminar (CU); A graduate course introducing students to cryptanalysis. Differential and linear cryptanalysis, square attack, RSA basics, factoring, protocol errors, lattices, Coppersmith's algorithm.

CSCI 7000 — Quantum Computing (CU); Introduction to quantum circuits, number theory, Shor's Algorithm, Grover's Algorithm.

Graduate Students

Rakhi Motwani, M.S., Completed: Spring 2002.

Scott Fritzinger, M.S., Completed: Summer 2002.

Hector Urtubia, M.S., Completed: Spring 2003.

Hiba Fayoumi, M.S., Completed: Summer 2004.

Mary Hedges, M.S., Completed: Spring 2007.

Joeshph Dunn, Ph.D., co-advisor with John Bennett, Completed: Summer 2007.

Martin Cochran, Ph.D., Completed: Spring 2008.

Jared Nishikawa, Ph.D., Completed: Spring 2016.

Undergraduate Students Troy Trimble, University of California at San Diego. REU Student, Summer 2003.
Gagan Sekhon, California State University at Hayward. REU Student, Summer 2003.
Ryan Gardner, University of Colorado at Boulder. REU Student, Summer 2004.
Trevor Highland, University of Texas at Austin. REU Student, Summer 2005.

**External
Service**

Secretary, International Association for Cryptologic Research, 2005–2007.
Program Committee, ACNS 2015.
Program Committee, CT-RSA 2015.
Program Committee, FSE 2014.
Program Committee, CT-RSA 2014.
Program Committee, CT-RSA 2013.
Program Committee, Eurocrypt 2012.
Program Committee, FSE 2011.
Program Committee, PKC 2011.
Program Committee, CANS 2010.
General Chair, CRYPTO 2009.
Program Committee, CRYPTO 2008.
Program Committee, ACNS 2008.
Program Committee, RSA-CT 2007.
Program Committee, ISC 2007.
Program Committee, ACNS 2007.
Program Committee, ACM CCS 2006.
Program Committee, CANS 2006.
Program Committee, ICISC 2006.
Program Committee, SECURE 2006.
Program Committee, ACSAC 2006.
Program Committee, CRYPTO 2005.
Program Committee, SAC 2005.
Program Committee, ICISC 2005.
Program Committee, CANS 2005.
Program Committee, IEEE SISW 2005.
Program Committee, CRYPTO 2004.
Program Committee, EUROCRYPT 2004.
Program Committee, RSA-CT 2003.
NSF CISE Panelist, 2001, 2003, 2005, 2006, 2007, 2009.
Referee for Journal of Cryptography, 1999–2006.
Referee for Software: Practice and Experience, 2005.
Referee for IEEE Communications Magazine, 2005.
Referee for IEEE Transactions on Circuits and Systems I, 2005.
Referee for IEEE Computer, 2005.
Referee for Journal of Computer Security, 2004.
Referee for IEEE Transactions on Information Theory, 2003.
Referee for IEEE Transactions on Computers, 2002.
Reviewer for CRYPTO 1999–2002, SODA 1998, SPAA 2002, Asiacrypt 2004, EUROCRYPT 2006.

Developed **CryptoStats** web site: an application which tracks publication rates by year, by author, by conference in the two main cryptography conferences. It was heavily used in my community (on average 240 hits per month), 2003–2009.

ACM Programming Contest problem composer, 2003–2007.
ACM Programming Contest site administrator, 2005.

Graduate Student Mixer organizer, CRYPTO 2005.

**Internal
Service**

Chair, Computing Committee, 2010–2011, 2012–2015.

Chair, Space Committee, 2012–2015.

Liaison, Casey Feldman Foundation, 2010–2015.

Member, Departmental Executive Committee, 2003–2005, 2007–2009, 2013–2015.

Member, Executive Committee, Computer and Communications Security Center, 2003–2006.

Member, Departmental Search Committee, 2003–2006, 2012–2014.

Chair, Departmental Search Committee, 2008–2009.

Member, Graduate Committee, 2005–2006.

Developed departmental voting software, now used for all departmental votes and college votes.